UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

OCENA STANDARDA VAROVANJA KOMUNIKACIJSKIH OMREŽIJ ISO 27033 GLEDE NA SODOBNE TRENDE NA PODROČJU INFORMACIJSKE VARNOSTI

Ljubljana, september 2015 URBAN ŠVARA

IZJAVA O AVTORSTVU

Spodaj podpisani Urban Švara, študent Ekonomske fakultete Univerze v Ljubljani, izjavljam, da sem avtor magistrskega dela z naslovom Ocena standarda varovanja komunikacijskih omrežij ISO 27033 glede na sodobne trende na področju informacijske varnosti, pripravljenega v sodelovanju s svetovalcem prof. dr. Tomažem Turkom.

Izrecno izjavljam, da v skladu z določili Zakona o avtorski in sorodnih pravicah (Ur. l. RS, št. 21/1995 s spremembami) dovolim objavo magistrskega dela na fakultetnih spletnih straneh.

S svojim podpisom zagotavljam, da

- je predloženo besedilo rezultat izključno mojega lastnega raziskovalnega dela;
- je predloženo besedilo jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem
    - poskrbel, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam v magistrskem delu, citirana oziroma navedena v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, in
    - pridobil vsa dovoljenja za uporabo avtorskih del, ki so v celoti (v pisni ali grafični obliki) uporabljena v tekstu, in sem to v besedilu tudi jasno zapisal;
- se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku (Ur. l. RS, št. 55/2008 s spremembami);
- se zavedam posledic, ki bi jih na osnovi predloženega magistrskega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom.

V Ljubljani, dne _____ Podpis avtorja:_____

KAZALO

KAZALO SLIK

KAZALO TABEL

UVOD

Danes si težko predstavljamo organizacijo brez informacijskega sistema, katerega velik del so tudi različna komunikacijska omrežja, po katerih se med posameznimi informacijskimi sistemi prenašajo podatki. Organizaciji ta omrežja omogočajo hiter dostop do podatkov in informacij, potrebnih za izvajanje poslovnih procesov, žal pa hkrati prinašajo tudi nova tveganja. Poleg odvisnosti poslovnih procesov organizacije od neprekinjenega delovanja omrežij so organizacije v vedno večji meri odvisne tudi od varnosti omrežij in posledično podatkov, ki se preko omrežij prenašajo ali so preko omrežij dostopni (International Organization for Standardization, 2009, str. VI). Pri vzpostavljanju učinkovite informacijske varnosti organizacije uporabljajo različne standarde in primere dobre prakse, saj je učenje na napakah lahko zelo drago, naložba v informacijsko varnost pa lahko hitro preseže njene koristi (Gordon & Loeb, 2002, str. 439). Med najbolj uporabljane standarde na tem področji spadajo standardi vodenja informacijske varnosti ISO/IEC družine 27000 (Susanto, Almunawar & Tuan, 2011, str. 26-27), katere del je tudi standard ISO/IEC 27033, ki obravnava varovanje komunikacijskih omrežij. Standard je razdeljen na 6 delov, ki določajo zahteve in smernice za varno upravljanje ter uporabo komunikacijskih omrežij (ISO, 2014, str. IV). Izdaje posameznih delov standarda so med letoma 2009 in 2014, kar nakazuje, da lahko posamezni deli standarda predlagajo varnostne nadzorne točke in ukrepe, ki danes ne zagotavljajo zadovoljivega nivoja varnosti.

Osnovni cilj magistrskega dela je ugotoviti ali je standard ISO/IEC 27033 dovolj široko ter dolgoročno usmerjen in se dopolnjuje ter osvežuje dovolj pogosto, da njegove smernice zagotavljajo učinkovito varovanje komunikacijskih omrežij pred najnovejšimi tehnikami napadov. Podcilji, preko katerih bom prišel do končnih ugotovitev, so opredelitev informacijske varnosti, analiza in predstavitev standarda ISO/IEC 27033, analiza sodobnih tipov in tehnik napadov, analiza sodobnih tehnik in tehnologij varovanja in pregled razkoraka med zahtevami standarda in sodobnimi tehnikami napadov ter varovanja komunikacijskih omrežij.

Raziskovalno vprašanje, na katerega bom odgovoril, je: ali zahteve in priporočila standarda ISO/IEC 27033 zagotavljajo učinkovito varovanje komunikacijskih omrežij glede na najsodobnejše tehnike napadov.

Metodologija raziskovanja temelji na pregledu strokovne literature in sintezi ugotovitev s pripravo priporočil, uporabil pa sem tudi številna znanja in izkušnje, ki sem jih pridobil v okviru dodiplomskega in podiplomskega študija ter pri sodelovanju pri različnih projektih, vezanih na komunikacijska omrežja in informacijsko varnost.

Magistrsko delo je sestavljeno iz petih poglavij. V poglavju št. 1 sem opisal različne tipe komunikacijskih omrežij ter predstavil osnovne tehnike in principe varovanja posameznega tipa komunikacijskega omrežja. V poglavju št. 2 sem predstavil sestavo standarda ISO/IEC 27033, analiziral, kaj posamezni del standarda obravnava in zapisal temeljne zahteve in priporočila posameznega dela standarda. V poglavju št. 3 sem opisal različne tipe napadov na omrežja,

najbolj pogoste motive napadov, analiziral različne tehnike izogibanja zaznavi napadov, analiziral najbolj odmevne ranljivosti in napade zadnjega leta ter analiziral dostopnost orodij za izvedbo tovrstnih napadov. V poglavju št. 4 sem predstavil sodobne tehnike in tehnologije varovanja komunikacijskih omrežij, analiziral povprečni čas odprave posameznih ranljivosti in analiziral uporabnost varnostnih preverjanj. V zadnjem poglavju sem analiziral razkorak med zahtevami in priporočili standarda ISO/IEC 27033 ter dejanskimi ukrepi, ki so potrebni za zagotavljanje zaščite komunikacijskih omrežij pred najnovejšimi tipi napadov z uporabo najnovejših tehnik in tehnologije za preprečevanje napadov na komunikacijska omrežja in informacijske sisteme.

1 VARNOST KOMUNIKACIJSKIH OMREŽIJ

Pomembnost komunikacijskih omrežij (v nadaljevanju omrežij) iz dneva v dan narašča, skladno s tem pa tudi pomembnost varovanja omrežij. Informacijske sisteme, ki jih organizacija potrebuje za svoje poslovanje, povezujejo različna omrežja, ki se v grobem delijo na notranje omrežje, povezovalna omrežja in javna omrežja. Notranje omrežje organizaciji zagotavlja dostope do lastnih informacijskih virov. Po njih se prenašajo podatki med uporabniki, informacijskimi viri organizacije ter informacijskimi viri povezanih omrežij. Povezovalna omrežja organizacijo povezujejo s poslovnimi enotami, poslovnimi partnerji, javnimi ustanovami itd. Ta omrežja organizaciji omogočajo dostop do informacijskih virov izven lastnega omrežja in povezovanje geografsko razpršenih omrežij organizacije. Javna omrežja, kot je na primer internet, organizaciji omogočajo dostop do javnih informacij, komunikacijo z drugimi organizacijami in strankami, elektronsko poslovanje, dostop do javnih storitev in podobno (Andress, 2014; Internet-Society, 2014; ISO, 2009).

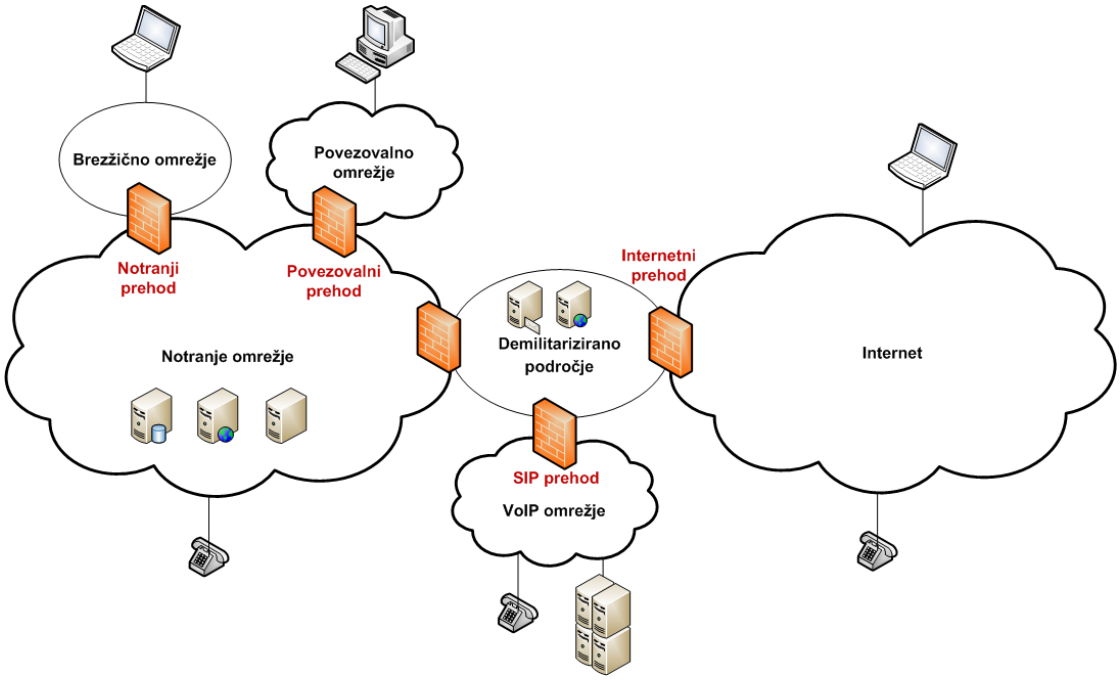
Organizacije lastno omrežje povezujejo z drugimi omrežji zaradi poslovnih zahtev. Vsa povezana omrežja jim omogočajo normalno poslovanje, izpad enega ali več omrežji pa lahko vpliva na doseganje poslovnih ciljev. Za uspešno poslovanje morajo organizacije zagotoviti neprekinjeno delovanje vseh lastnih omrežij ter nadomestne poti in postopke dela ob izpadu omrežij, od katerih je organizacija odvisna, a z njimi ne upravlja sama. Za organizacijo pa ni pomembno zgolj delovanje posameznega omrežja. Ker imajo organizacije dostop do različno klasificiranih podatkov in informacij, lahko nepooblaščeno razkritje le-teh negativno vpliva na dobro ime organizacije, pripelje do kazenske odgovornosti, ali celo ogrozi obstoj organizacije. Poleg delovanja omrežij je zelo pomembna tudi njihova varnost ter posledično varnost podatkov, ki se po omrežjih prenašajo.

1.1 Kaj so komunikacijska omrežja

Po Hekmatu (2005, str. 1) je komunikacijsko omrežje infrastruktura, ki omogoča povezovanje dveh ali več naprav, ki so preko omrežja sposobne pošiljati in prejemati podatke. Omrežje sestavljajo vozlišča, gostiteljski računalniki in povezave med njimi. Hekmat (2005, str. 2-4) omrežja deli na več tipov oziroma kategorij glede na štiri merila: geografska razpršenost vozlišč

in gostiteljev, omejitev dostopa, komunikacijski model in model komutacije. Geografsko se danes omrežja delijo na osebna, lokalna in prostrana. Z vidika omejitve dostopa se delijo na zasebna in javna, z vidika namena pa na omrežja organizacije, navidezna zasebna omrežja in pomnilniška omrežja. Komunikacijski model omrežja določa, ali je omrežje točkovnega tipa ali tipa razpršenega oddajanja, komutacija omrežja pa omrežja deli na paketna in vodovna (Hekmat, 2005; ISO, 2009). Na sliki 1 je prikazano klasično omrežje organizacije, ki ga sestavljajo notranje omrežje, brezžično omrežje, povezovalno omrežje, omrežje internetne telefonije, demilitarizirano področje ter povezava z internetom.

Slika 1: Primer komunikacijskega omrežja organizacije



Vir: ISO, ISO/IEC 27033-4:2014, 2014, str.5.

Ključnega pomena pri komunikaciji med napravami znotraj omrežja je komunikacijski protokol. Vse naprave, ki si morajo med seboj izmenjevati podatke, morajo za medsebojno komunikacijo uporabljati isti komunikacijski protokol. Danes je večina omrežij zgrajena z uporabo internetnega protokola (v nadaljevanju IP protokol), prav tako pa na tem protokolu temelji tudi največje javno omrežje, internet. Internet organizacije zaradi njegove razširjenosti in cenovno ugodnega dostopa uporabljajo za medsebojno povezovanje ter nudenje različnih storitev in komunikacijo s strankami. Slaba stran interneta pa je njegova zelo nizka privzeta varnost in zanesljivost. Če organizacija potrebuje povezavo z visoko stopnjo privzete varnosti in zanesljivosti, mora uporabiti dražje možnosti povezovanja. To sta na primer najem fizične povezave med poslovno enoto in organizacijo ali najem navidezne povezave preko skupne infrastrukture telekomunikacijskega operaterja. Slednja je finančno bolj ugodna, ker ne zahteva vzpostavljanja dragega fizičnega omrežja med posameznimi lokacijami. Operaterji za zagotavljanje povezljivosti uporabijo lastno infrastrukturo, povezave med lokacijami pa med seboj navidezno ločijo z uporabo različnih transportnih protokolov, kot je na primer MPLS. Ta

protokol omogoča vzpostavitev navideznih zasebnih omrežij preko fizičnega omrežja z označevanjem paketov, vsebuje pa tudi mehanizme za zagotavljanje minimalne propustnosti navidezne povezave. Za organizacijo je uporaba takšne povezave pregledna in enostavna, pri tem pa se mora zavedati tudi različnih varnostnih pomanjkljivosti takšnih povezav. Ker same po sebi ne zagotavljajo šifriranja, so z vidika varnosti sicer veliko bolj varne kot uporaba interneta, a manj varne kot najete fizične povezave. Organizacija mora zato sama poskrbeti za šifriranje komunikacije in morebitne obvodne poti za primere izpadov (Internet Engineering Task Force, 1999; ISO, 2009).

Poleg IP omrežij večje organizacije uporabljajo tudi pomnilniška omrežja (v nadaljevanju SAN omrežja). Ta omogočajo dostop posameznih informacijskih sistemov do skupnega pomnilniškega medija oziroma diskovnega sistema. Sestavljena so iz namenskih diskovnih sistemov in stikal, na katera so priključeni odjemalci. Za medsebojno komunikacijo naprave uporabljajo protokol optičnega kanala (v nadaljevanju FC). Ker so tovrstna omrežja zelo draga, v veljavo stopajo različni protokoli, ki omogočajo dostop do skupnih pomnilniških medijev preko IP omrežij. Najbolj znana protokola sta iSCSI in FCoE, ki omogočata izvajanje blokovnih ukazov SCSI in FC protokola preko IP omrežja, ki pa mora biti za takšno uporabo tudi pravilno zasnovano (ISO, 2009; Lee, 2014).

Zaradi odvisnosti poslovanja od delovanja in varnosti omrežij, morajo organizacije le-ta varovati pred nepredvidenimi izpadi in nepooblaščenim dostopom do omrežnih sistemov ter podatkov, ki se po omrežjih prenašajo. Osnovne principe varovanja komunikacijskih omrežij bom predstavil v naslednji točki.

1.2 Osnovni principi varovanja omrežij

Omrežja varujemo z organizacijskimi in tehničnimi kontrolami, ki jih navadno predpisuje varnostna politika omrežja organizacije. Varno omrežje mora zagotavljati zaupnost, celovitost in razpoložljivost omrežja ter preko omrežja dosegljivih naprav, informacijskih sistemov, storitev, aplikacij in podatkov. V osnovi pri tem govorimo o overjanju dostopov do omrežja in omrežnih virov, ki ga je treba izvajati na vseh nivojih, od fizičnega do aplikacijskega, da se s tem zaščitijo elementi omrežja pred raznovrstnimi napadi (Pawar & Anuradha, 2015, str. 503-506). Napadi se po Andressu (2014, str. 8) delijo na štiri kategorije: prestrezanje, spreminjanje, ponarejanje in prekinitev. Vsaka kategorija zahteva svoj način varovanja.

Napadi v kategoriji prestrezanja vplivajo na zaupnost komunikacije, njihov cilj pa je pridobitev neavtoriziranega dostopa do podatkov, ki se prenašajo po omrežju. Izvedba napada zahteva neposreden dostop napadalca do opreme ali povezav v omrežju in ga je načeloma težko zaznati, saj pri tem napadalci aktivno ne posegajo v delovanje omrežja in podatkovni tok. Varovanje pred takšnimi napadi zahteva varovanje fizičnega nivoja omrežne infrastrukture, torej bakrenih, optičnih in brezžičnih povezav ter vseh priključkov, dostopnih točk in aktivne omrežne opreme, ki omrežje sestavljajo. Posebno pozornost je treba nameniti tudi varnosti dostopov do aktivne

omrežne opreme, saj je prestrezanje podatkov v veliki večini ena od osnovnih funkcionalnosti takšne opreme. Dostop do tovrstne opreme bi napadalcu lahko omogočil tudi oddaljeno prestrezanje podatkov (Andress, 2014; Pawar & Anuradha, 2015).

Napadi v kategoriji spreminjanja lahko vplivajo na različne vire organizacije in posledično na zaupnost, celovitost in razpoložljivost le-teh. Cilj tovrstnih napadov je izvesti spremembo nastavitev aktivne opreme znotraj omrežja, s čimer napadalec vpliva na integriteto nastavitev in naprave same. Uspešna sprememba nastavitev stikala ali usmerjevalnika lahko omogoči tudi prestrezanje prometa, kar posledično vpliva na zaupnost komunikacije, izklop naprave pa vpliva na razpoložljivost omrežja (Andress, 2014, str. 8-9). Varovanje pred tovrstnimi napadi zahteva uporabo varnih načinov overjanja uporabnikov in skrbnikov, segmentiranje uporabniških in skrbniških omrežij ter šifriranje povezav (ISO, 2012, str. 5-6).

Napadi v kategoriji ponarejanja vplivajo na celovitost in razpoložljivost. Napadalec lahko na primer s ponarejanjem elektronske pošte poskuša uporabnike prelisičiti v namestitev zlonamerne programske opreme, ki mu iz okuženega sistema posreduje zahtevane podatke ali pa mu celo omogoči oddaljeni dostop do sistema. Zaščito pred tovrstnimi napadi omogoča preverjanje istovetnosti, overjanje dostopa, pregledovanje vsebine komunikacije in šifriranje povezav. Primer napadov s ponarejanjem, ki vplivajo na razpoložljivost, so napadi onemogočanja storitve in porazdeljeni napadi onemogočanja storitve. Pri teh napadih napadalec z ustvarjanjem posebno narejenih IP paketov, usmerjenih na neko storitev organizacije, usmerjevalnika ali varnostnega prehoda, poskuša z izčrpavanjem virov na ciljnem sistemu ali omrežju doseči njegov izpad. Pred takimi napadi se organizacije branijo predvsem s sistemi za preprečevanje vdorov, aplikacijskimi požarnimi pregradami in posredniški strežniki. Težje pa se organizacija obrani napada, ki z ustvarjanjem velike količine IP paketov vpliva na propustnost določene povezave med dvema omrežjema in tako doseže izpad dostopa do ciljnega omrežja. Cilj takšnih napadov je navadno povezava med organizacijo in internetom, obrambo pred tem napadom pa lahko zagotovi le ponudnik dostopa do interneta, ki zlonamerne IP pakete prestreže, preden so posredovani proti povezavi med ponudnikom in organizacijo. To pomeni, da mora imeti organizacija za obrambo pred takšnimi napadi vzpostavljen postopek komunikacije s ponudnikom, ki bo ta napad tudi prestregel (Andress, 2014; Hekmat, 2005; ISO, 2009, 2010, 2012).

Kategorija prekinitev vsebuje napade, s katerimi lahko napadalci onemogočijo izvajanje storitve, posamezno povezavo, del omrežja ali celotno omrežje organizacije. To lahko izvedejo na načine, ki so bili opisani v prejšnjih kategorijah. Osnovni principi zaščite pred tovrstnimi napadi so preverjanje istovetnosti, overjanje dostopa, pregledovanje vsebine, šifriranje povezav in vzpostavitev postopka komunikacije s ponudniki dostopov do javnih omrežij (Akhgar & Arabnia, 2013; Andress, 2014; ISO, 2009, 2010, 2012).

Podrobneje bom principe varovanja opisal v točki 4.1, v nadaljevanju pa bom na kratko opisal, kaj so sestavni deli posameznega omrežja in kaj je v posameznih omrežjih treba varovati.

1.3 Kaj varujemo v posameznih omrežjih

V omrežjih je treba varovati podatke in storitve, ki nam jih nudi informacijski sistem. Pogoj za njihovo varnost je varnost omrežne opreme, ki sestavlja omrežje, naprav, ki skrbijo za varnost omrežja ter sistemov, ki uporabnikom nudijo različne storitve izmenjave ter dostopa do podatkov in informacij.

Zunanje omrežje organizacije sestavljajo povezave s ponudniki dostopov do javnih omrežij, morebitne povezave z omrežji drugih organizacij in tako imenovana demilitarizirana področja. Demilitarizirano področje (v nadaljevanju DMZ področje) je posebno, od ostalih delov omrežja ločeno omrežje, v katerem organizacije navadno gostijo strežnike in storitve, ki zahtevajo višjo varnost ali morajo biti izpostavljene drugim organizacijam in dostopom iz javnih omrežij. Te naprave so ločene od omrežja organizacije prav zaradi svoje izpostavljenosti manj varnim omrežjem, s čimer organizacija ob morebitnem vdoru napadalcev prepreči neposredno izpostavljenost bolj varnih omrežij napadalcem. Naprave, ki sestavljajo zunanje omrežje, so navadno usmerjevalniki, brezžični usmerjevalniki, požarne pregrade, posredniški strežniki, sistemi za navidezna zasebna omrežja, sistemi za zaznavanje in preprečevanje vdorov, omrežna stikala in pretvorniki medijev. Ker te naprave omogočajo delovanje omrežij in omrežnih povezav, je njihova varnost predpogoj za varnost strežnikov in storitev v DMZ področjih ter notranjih omrežjih organizacije. Omrežne naprave za svoje delovanje potrebujejo natančne nastavitve, ki jih je moč spreminjati preko konzolnega dostopa neposredno na napravi ali preko oddaljenega omrežnega dostopa. Njihova varnost je torej odvisna od fizične varnosti naprave in varnosti omrežnega nastavitvenega vmesnika, zagotoviti pa jo je treba z overjanjem fizičnih in logičnih dostopov, šifriranjem komunikacije med omrežno napravo in delovno postajo skrbnika ter omejevanjem možnosti dostopa do nastavitvenega vmesnika naprave iz točno določenih delovnih postaj skrbnikov (Andress, 2014; Pawar & Anuradha, 2015).

Notranje omrežje, podobno kot zunanje, navadno sestavljajo usmerjevalniki, požarne pregrade, sistemi za zaznavanje in preprečevanje vdorov, brezžične dostopne točke, omrežna stikala itd., ki jih varujemo na enak način kot naprave v DMZ področju. Poleg teh naprav pa je treba v notranjem omrežju varovati tudi večje število strežnikov in storitev, delovnih postaj uporabnikov, tiskalnikov, sistemov pristopne kontrole, sistemov za zagotavljanje brezprekinitvenega napajanja, pomnilniških sistemov, raznih industrijskih sistemov itd. Tako kot je od delovanja omrežja odvisna sposobnost medsebojne komunikacije naštetih naprav, je tudi delovanje omrežja odvisno od pravilnega delovanja naprav v omrežju. Za zagotavljanje varnosti je treba tudi te naprave varovati pred nepooblaščenim dostopom in napadi iz zunanjih omrežij, notranjih omrežij ter morebitnih navideznih zasebnih povezav, ki omogočajo oddaljene dostope do omrežja organizacije in naprav znotraj tega omrežja (Hekmat, 2005; Internet-Society, 2014; ISO, 2009).

Veliko manjši nabor različnih naprav pa sestavlja pomnilniška omrežja. Te naprave so diskovni sistemi in omrežna stikala, na katera so priključeni odjemalci. V teh omrežjih je treba varovati

predvsem fizične povezave, diskovne sisteme in omrežna stikala z omejevanjem fizičnega in logičnega dostopa do opreme ter omrežnega nastavitvenega vmesnika (Lee, 2014, str. 140-143).

Z vzpostavljanjem kompleksnih omrežij in z njihovo vedno večjo odvisnostjo od varnosti organizacije uporabljajo različne varnostne standarde v upanju, da bodo z uvedbo predpisanih varnostnih kontrol dosegle visoko stopnjo varnosti lastne informacijske in komunikacijske infrastrukture (Susanto et al., 2011, str. 21-22). V nadaljevanju bom analiziral standard ISO/IEC 27033, katerega namen je vzpostavitev učinkovitega varovanja komunikacijskih omrežij.

2 STANDARD ISO/IEC 27033

Standard ISO/IEC 27033 je del družine standardov ISO/IEC 27000, ki spada med najbolj uporabljano družino standardov za informacijsko varnost (Susanto et al., 2011, str. 26). Namen standardov te družine je, da organizacijam dajejo smernice, zahteve ter primere dobre prakse za varovanje informacijskih sredstev v vseh digitalnih in fizičnih oblikah. Standard ISO/IEC 27033 podaja smernice za izvedbo varnostnih kontrol za vzpostavitev učinkovitega varovanja komunikacijskih omrežij in je zasnovan kot nadgradnja standardov ISO/IEC 27002 in ISO/IEC 27005 (ISO, 2009, str. V-VII).

2.1 Obseg in struktura standarda

Prvi del standarda, ISO/IEC 27033-1, v uvodu opredeljuje obseg in strukturo celotnega standarda. Z naraščanjem pomembnosti različnih tipov omrežij se morajo novodobne organizacije spopadati tudi z novimi vrstami tveganj, ki jih vsa ta medsebojno povezana omrežja prinašajo. Kot to določajo tudi drugi standardi varovanja informacij, morajo organizacije zagotoviti dostopnost, zaupnost in integriteto informacij, od katerih je organizacija odvisna (ISO, 2009, 2013a, 2013b). Standard ISO/IEC 27033 obravnava varnost omrežij, ki omogočajo prenos podatkov med različnimi točkami v informacijskem sistemu organizacije. Prenos podatkov se lahko izvaja med posameznimi informacijskimi sistemi, uporabniki in informacijskimi sistemi ter med posameznimi uporabniki oziroma njihovimi napravami, priključenimi v omrežje organizacije. Standard opisuje in opredeljuje smernice, zahteve in primere dobre prakse, ki skrbnikom in arhitektom omrežij omogočajo vzpostavitev varnih omrežij znotraj organizacije, med organizacijami in med zunanjimi uporabniki ter organizacijo (ISO, 2009, str. 1).

Prvič je bil standard s splošnim nazivom Informacijska tehnologija – tehnike varovanja – varovanje IT omrežij izdan leta 2006, in sicer v seriji ISO 18000, s številko 18028. Po strukturi je bil takrat standard razdeljen na pet delov. Leta 2009 je bila na njegovi podlagi izdana nova različica standarda varovanja IT omrežij v seriji ISO standardov 27000 s številko 27033-1. Novi standard je predvideval sedem delov (ISO, 2009, str. IV-VII, 10):

a) 27033-1: Pregled in koncepti,
b) 27033-2: Smernice za zasnovo in izvedbo varovanja omrežij,
c) 27033-3: Tveganja, tehnike načrtovanja in problemi nadzora za referenčna omrežja,
d) 27033-4: Tveganja, tehnike načrtovanja in problemi nadzora pri varovanju komunikacij med omrežji z uporabo varnih prehodov,
e) 27033-5: Tveganja, tehnike načrtovanja in problemi nadzora pri varovanju navideznih zasebnih omrežij,
f) 27033-6: IP konvergenca in
g) 27033-7: Brezžična omrežja.

Do tretje spremembe strukture standarda je prišlo leta 2013, ko je bil izdan peti del standarda: ISO/IEC 27033-5. Standard se trenutno deli na šest delov, izdanih pa je le prvih pet delov. Nova struktura standarda in obseg posameznega dela standarda sta (ISO, 2013c, 2014):

a) ISO/IEC 27033-1 opredeljuje koncepte in smernice za upravljanje varovanja omrežij.
b) ISO/IEC 27033-2 podaja organizacijam smernice za načrtovanje, oblikovanje in izvajanje varovanja omrežij.
c) ISO/IEC 27033-3 preko primerov referenčnih omrežij opisuje tveganja, tehnike oblikovanja in probleme nadzora.
d) ISO/IEC 27033-4 podaja smernice za zaščito komunikacij med omrežji z uporabo varnostnih prehodov, kot na primer požarnih pregrad, usmerjevalnikov, sistemov za preprečevanje vdorov itd., v skladu z varnostno politiko organizacije.
e) ISO/IEC 27033-5 podaja smernice za izbor, izvedbo in spremljanje tehničnih kontrol, potrebnih za zagotavljanje varnosti povezav med omrežji in uporabniki z uporabo navideznih zasebnih omrežij.
f) Zadnji del standarda, ISO/IEC 27033-6, ki je še v pripravi, pa bo obravnaval varnost brezžičnih omrežij.

Posamezen del standarda obravnava dodeljen tehnični odbor in vsak del ima svoj življenjski cikel. To pomeni, da je vsak del standarda izdan neodvisno od drugih delov, celotni standard pa se pripravlja preko več let. Nekateri deli standarda, ki obravnavajo določeno tematiko varovanja komunikacijskih omrežij, so tako novejši kot drugi in posledično obravnavajo novejše principe varovanja. Če pogledamo samo časovni razkorak med trenutno izdanimi deli standarda, je bil prvi del izdan leta 2009, drugi del leta 2012, tretji del leta 2010, četrti del leta 2014 in peti del leta 2013. Zadnji, šesti del, je v fazi pregleda in je predviden za izdajo v letu 2016 (ISO, b.l.).

V nadaljevanju magistrskega dela bom opisal vsak že izdani del standarda, njegov obseg, strukturo, priporočila in zahteve.

2.2 ISO/IEC 27033-1:2009

Prvi del standarda, ISO/IEC 27033-1:2009, nosi naziv Pregled in koncepti in je prva izdaja

prvega dela standarda v skupini 27033. Povzet je bil po standardu ISO/IEC 18028-1, ki je bil izdan leta 2006 in ga v celoti zamenjuje. Trenutno je v pripravi druga izdaja standarda, ki naj bi izšla v letu 2015 (ISO, b.l.).

2.2.1 Obseg in struktura

Standard nam podaja pregled standarda ISO/IEC 27033 s pregledom omrežne varnosti in opredelitvijo konceptov za upravljanje varovanja omrežij ter s tem povezanih definicij. Standard definira omrežno varnost kot obseg varovanja celotnega omrežja, torej varovanje omrežnih naprav, upravljanja omrežnih naprav, aplikacij oziroma storitev in končnih uporabnikov ter varovanja podatkov, ki se prenašajo po omrežju. Obseg standarda zajema tudi smernice za identifikacijo in analizo tveganj, povezanih z omrežno varnostjo ter na podlagi rezultatov analize predlaga zahteve za vzpostavitev omrežne varnosti. Ker različne tehnične varnostne arhitekture zahtevajo drugačen pristop, nam standard predlaga tudi pregled tehničnih kontrol za posamezno varnostno arhitekturo, ki pa se poleg omrežij nanašajo tudi ne druge vidike zagotavljanja informacijske varnosti. Ker je visoka kakovost tehnične varnostne arhitekture omrežja zelo pomembna, nam standard v tem delu podaja tudi pregled načinov za njeno doseganje in predstavi različna tveganja, zasnovo in vidike kontrol, povezanih z referenčnimi omrežji in tehnologijami omrežij, ki so detajlno predstavljena v tretjem delu standarda. V zadnjih točkah nam podaja še kratek pregled različnih vprašanj, povezanih z izvedbo, upravljanjem omrežnih varnostnih kontrol in njihovega stalnega nadzorovanja ter pregledovanja izvajanja. Prvi del standarda tako ni namenjen le skrbnikom, upravljavcem in arhitektom omrežij ter informacijske varnosti, temveč tudi vsem uporabnikom omrežij ter vodstvu organizacije, da lahko s pomočjo standarda bolje razumejo, zakaj je varnost komunikacijskih omrežij pomembna ter kaj in kako je v komunikacijskih omrežjih treba varovati (ISO, 2009, str. 1).

Prvi del standarda sestavlja pet uvodnih poglavij in devet poglavij, ki obravnavajo različne tematike varovanja omrežij. Šesto poglavje prvega dela standarda predstavlja pristop k omrežni varnosti s predstavitvijo ozadja ter procesom načrtovanja in upravljanja omrežne varnosti. Sedmo poglavje govori o prepoznavanju tveganj in pripravi na identifikacijo varnostnih kontrol z analizo obstoječega in načrtovanega omrežja ter analize varnostnih tveganj in identifikacijo potencialnih področij kontrol. Osmo poglavje predstavlja pregled kontrol, ki se nanašajo na omrežno varnost. Govori o upravljanju omrežne varnosti oziroma varnem upravljanju omrežne infrastrukture, upravljanju tehničnih ranljivosti omrežja, identifikaciji in preverjanju identitete uporabnikov omrežij, nadzoru nad delovanjem omrežja, hrambi revizijskih zapisov, zaznavanju in preprečevanju napadov, zaščiti pred škodljivo kodo, kriptografskih storitvah in upravljanju neprekinjenega poslovanja. Deveto poglavje podaja smernice za snovanje in izvedbo omrežne varnosti s predstavitvijo različnih vidikov tehničnih varnostnih arhitektur in zasnov omrežij ter pripadajočih kontrol. Deseto poglavje predstavlja tveganja, zasnovo, tehnike in probleme kontrol referenčnih omrežij v tehničnem smislu. Obravnava različna referenčna omrežja, ki odražajo različne povezave med sistemi in njihovimi uporabniki, od dostopa do interneta,

segmentacije omrežij, mobilnih komunikacij, oddaljenih dostopov itd. Enajsto poglavje je kazalo po prilogi A standarda 27033-1, ki opisuje različne tehnološke tematike, kot na primer lokalna omrežja, brezžična omrežja, navidezna omrežja itd. Dvanajsto poglavje opisuje pristop k razvoju in testiranju omrežij, trinajsto in štirinajsto poglavje pa na kratko opomnita na proces nenehnega izboljševanja, v katerem zahtevata stalno nadzorovanje varnosti omrežja, ukrepanje ob spremembah, novo načrtovanje in izvedbo pripadajočega testiranja sprememb ter izvedbo sprememb. Sestavni del prvega dela standarda so tudi tri priloge. Priloga A vsebuje opis različnih tveganj, tehnik snovanja in vprašanja kontrol glede na določeno tehnologijo oziroma tip omrežja. Priloga B podaja kazalnik oziroma sklice med standardi ISO/IEC 27001, ISO/IEC 27002 ter ISO/IEC 27033. Zadnja priloga, priloga C, pa je predolga dokumenta za upravljanje varovanja omrežij (ISO, 2009).

2.2.2 Priporočila in zahteve

Priporočila in zahteve prvega dela standarda so zapisane v devetih poglavjih in so splošne narave. V posameznem delu se standard sklicuje tudi na druge dele standarda, kjer so predstavljena tudi tehnična priporočila in zahteve.

2.2.2.1 Načrtovanje in upravljanje omrežne varnosti

V tem poglavju standard poudarja, da mora organizacija za vsako povezavo v omrežju poznati poslovne zahteve in koristi ter z njimi povezana varnostna tveganja, varnostno tehnično arhitekturo in področja varnostnih kontrol (ISO, 2009, str. 12). Pri pripravi načrta predlaga šest korakov.

V prvem koraku je treba določiti obseg oziroma okvir omrežja ter oceniti varnostna tveganja. Prva faza je zbiranje vseh potrebnih informacij. To sestavlja analiza varnostne politike organizacije in načrtovanje vseh varnostnih kontrol omrežja, zbiranje informacij o obstoječem omrežju ter pripravo dokumenta z načrtom novega omrežja. Načrt mora vsebovati vse značilnosti omrežja, kot na primer arhitekturo omrežja, aplikacije, storitve, tipe povezav itd. Poleg teh informacij je treba zbrati tudi informacije o grožnjah in ranljivostih, ki lahko vplivajo na poslovne procese organizacije. Druga faza je opredelitev in ocena varnostnih tveganj ter z njimi povezanih področij kontrole z upoštevanjem varnostnih zahtev referenčnih omrežij opisanih v 10. in 11. poglavju tega dela standarda (op. poglavji 2.2.2.5 in 2.2.2.6 v magistrskem delu).

V drugem koraku je treba opredeliti podporne tehnične in ne-tehnične kontrole, ki se poleg omrežne varnosti navezujejo tudi na splošno informacijsko varnost.

V tretjem koraku standard zahteva ovrednotenje zahtevane tehnične varnostne arhitekture in z njo povezanih kontrol z upoštevanjem scenarijev tehnične varnostne arhitekture ter zasnov, ki so opisane v poglavjih 9, 10, 11 ter prilogi A (op. poglavja 2.2.2.4, 2.2.2.5 in 2.2.2.6 v

magistrskem delu). Na podlagi ovrednotenja je treba pripraviti dokument z opisom izbrane arhitekture ter z njo povezanih varnostnih kontrol.

Zadnji korak je še razvoj in testiranje izbrane rešitve, izvedba in upravljanje varnostnih kontrol ter spremljanje in revidiranje izvedbe, detajlni koraki za to pa so opisani v poglavjih 12, 13 in 14 (op. poglavja 2.2.2.7, 2.2.2.8 in 2.2.2.9 v magistrskem delu) (ISO, 2009, str. 12-14).

2.2.2.2 Prepoznavanje tveganj in priprava na identifikacijo varnostnih kontrol

To poglavje standarda je namenjeno prepoznavanju in ocenjevanju tveganj, povezanih z omrežji in pripravo na identifikacijo varnostnih kontrol. Organizacija mora pri tem zbrati vse informacije o obstoječem in načrtovanem omrežju ter na njihovi podlagi identificirati in oceniti varnostna tveganja povezana z omrežjem, glede na katera bo lahko nato predvidela primerna območja kontrol (ISO, 2009, str. 14).

Prvi del je prepoznavanje varnostnih zahtev politike varovanja informacij organizacije, ki je ključen pri prepoznavanju tveganj, povezanih z omrežji in pri pripravi varnostnih kontrol. Politika varovanja informacij naj bi vsebovala priporočila in zahteve za zagotavljanje zaupnosti, integritete, preprečevanja zanikanja istovetnosti (angl. *non-repudiation)* sporočila in dostopnosti informacij ter posledično omrežij, ki omogočajo prenašanje in dostop do teh informacij. Stopnja tveganja, ocenjena v tem dokumentu, bo posledično tudi minimalna stopnja tveganja dela omrežja, ki zagotavlja tovrstne dostope. To bo podlaga za določanje varnostnih zahtev posameznih delov omrežja, kot so na primer način dostopa do omrežja in varovanje komunikacij s tem omrežjem ali na primer zahteve po kriptografskih metodah pri prenosu ali hrambi posameznih podatkov in informacij. Vse te zahteve morajo biti zbrane in zapisane v dokumentu, ki določa minimalne zahteve po varnostni arhitekturi in potencialnih področjih kontrole (ISO, 2009, str. 15).

Drugi del je namenjen zbiranju informacij o obstoječih in načrtovanih omrežjih, na podlagi katerih lahko organizacija ocenil tveganja in minimalne varnostne zahteve, ki jih bo morala podpirati arhitektura omrežja organizacije. Prvi korak je zbiranje informacij o omrežni arhitekturi, aplikacijah in storitvah. V tem koraku je treba zbrati podrobnosti o obstoječi in načrtovani omrežni arhitekturi, aplikacijah in storitvah. Te so pogoj za razumevanje in specifikacijo okvirov okolja organizacije, na podlagi katerih se lahko izvede analiza varnostnih tveganj in izbere primerno varnostno arhitekturo omrežja. V sklopu zbiranja podatkov in analize je treba določiti tipe omrežij, ki jih organizacija uporablja, s katerimi drugimi omrežji je organizacija povezana in na kakšen način ter kakšne dostope iz zunanjih omrežij varnostna politika sploh dovoljuje. Izvesti mora tudi analizo in pregled različnih protokolov, ki jih načrtuje uporabiti v svojem omrežju. Kot primer teh protokolov standard podaja protokole za souporabo, protokole za identifikacijo in nadzor dostopa, usmerjevalne protokole in transportne protokole. Za vsak protokol mora organizacija dobro poznati njegove varnostne vidike, pri tem pa mora upoštevati tudi tip medija, po katerem se prenašajo podatki, saj je treba brezžične

komunikacije drugače obravnavati kot ožičena omrežja. Standard v tem koraku zahteva poleg analize omrežij tudi analizo aplikacij in storitev, ki so dostopne preko omrežja in so ključnega pomena za poslovne procese organizacije. Te aplikacije in storitve so lahko lahki odjemalci, namizne aplikacije, terminalni dostopi, infrastruktura in aplikacije za prenašanje sporočil, odjemalec-strežnik aplikacije, aplikacije za posredovanje podatkov in krmiljenje naprav itd. Za posamezno aplikacijo je treba analizirati vse varnostne zahteve, ki jih aplikacija potrebuje za varno delovanje. Standard kot primer podaja šifriranje komunikacije pri prenašanju sporočil, podpisovanje prenosne kode za lahke odjemalce in varovanje podatkov med prenašanjem pri uporabi aplikacij za posredovanje podatkov in krmiljenje. V enak kontekst zahtev spadajo tudi različne storitve, kot na primer sistemi domenskih imen, elektronski pošti, prenos govora preko IP omrežij itd. (ISO, 2009, str. 15-17).

Drugi korak je identifikacija tipov omrežnih povezav, ki organizaciji nudijo povezovanje z drugimi in svojimi omrežji. Na podlagi kategorije je treba izvesti analizo varnostnih tveganj in pripraviti predlog pripadajočih varnostnih kontrol ter tehnične varnostne arhitekture omrežja. Standard predlaga kategorizacijo povezav na povezave med različnimi točkami omrežja znotraj poslovne stavbe, povezave med geografsko oddaljenimi točkami omrežja organizacije, ki lahko tudi omejujejo dostop do določenih delov komunikacijskega omrežja iz oddaljene točke, povezave med uporabniki, ki uporabljajo oddaljeni dostop do omrežja organizacije, povezave z organizacijami zaprte skupnosti, kot na primer partnerskimi organizacijami, bankami ali organizacijami, ki jim dostop do informacijskega sistema organizacije določa zakon, povezave z ostalimi organizacijami, ki omogočajo dostope do različnih podatkov in informacij, kot na primer raziskovalne institucije, organizacije, ki nudijo razne statistične podatke itd, povezave z domenami splošne javnosti, ki jih vzpostavijo uporabniki znotraj organizacije, kot na primer dostopi do javnih podatkovnih baz, elektronska pošta, spletne strani itd in povezave s ponudnikom javnega telefonskega omrežja (ISO, 2009, str. 17-18).

Za vsako od povezanih omrežij je treba definirati tudi ostale karakteristike, ki lahko vplivajo na varnost in delovanje omrežja. To vključuje razlikovanje med javnimi in zasebnimi omrežji, razlikovanje glede na tip podatkov, ki omrežja deli na podatkovna, govorna in hibridna omrežja, ločevanje glede na tip omrežij, ki omrežja deli na ločevanje paketno, komutirano in MPLS omrežje, specifikacijo minimalne propustnosti in zakasnitev v omrežju, morebitne zahteve po zagotavljanju kakovosti storitve ter specifikacijo povezave do omrežja, torej ali gre za trajno povezavo ali pa se vzpostavlja po potrebi. Ko zberemo zgoraj napisane specifikacije, standard (ISO, 2009, str. 18-19) za lažjo oceno varnostnih tveganj priporoča še klasifikacijo omrežij glede na uporabnike:

a) neznana omrežna skupnost uporabnikov, ki uporabljajo zasebno omrežje,
b) omrežna skupnost uporabnikov znotraj poslovne skupnosti več organizacij, ki uporabljajo zasebno omrežje,
c) omrežna skupnost uporabnikov znotraj ene organizacije, ki uporabljajo zasebno omrežje,
d) neznana omrežna skupnost uporabnikov, ki uporabljajo javno omrežje,

e) omrežna skupnost uporabnikov znotraj poslovne skupnosti več organizacij, ki uporabljajo javno omrežje in
f) omrežna skupnost uporabnikov znotraj ene organizacije, ki uporabljajo javno omrežje.

Taka klasifikacija bo organizaciji v pomoč pri določanju specifičnih varnostnih tveganj glede na tip omrežja in tipa skupnosti uporabnikov ter posledično vplivala na arhitekturo omrežja. Kot zadnjo točko standard predlaga zbiranje ostalih informacij, ki so potrebne za oceno tveganja in varnostno presojo po standardih ISO/IEC 27001 in ISO/IEC 27002. Te vključujejo poslovne procese, tip informacij, uporabljene in načrtovane komponente strojne in programske opreme, storitve, povezave itd., lokacije in prostore komunikacijske opreme ter aktivnosti oziroma operacije (ISO, 2009, str. 19).

Zadnji korak pri zbiranju informacij o obstoječih in načrtovanih omrežjih je analiza varnostnih tveganj in potencialnih področij za nadzor, s čimer preprečimo izpostavljanje uporabnikov, informacijskih sistemov in podatkov novim tveganjem. Pri tem je treba upoštevati tudi tveganja, povezana z zagotavljanjem skladnosti z aktualno zakonodajo, saj ta lahko za določeno vrsto podatkov definira tudi minimalne varnostne zahteve. Tveganja je treba oceniti glede na izpostavljenost informacij nepooblaščenemu dostopu, nepooblaščenemu posredovanju, vnosu zlonamerne kode, ohromitvi oziroma zavračanju pošiljatelja ali prejemnika, ohromitvi oziroma zavračanju storitve in nedosegljivost informacij ali storitve. Ta tveganja po standardu lahko vplivajo na zaupnost in integriteto informacij in kode med prenosom preko omrežij in stanju mirovanja na sistemu, ki je priključen na omrežje; razpoložljivost informacij in omrežnih storitev ter sistemov, ki so povezani na omrežje; preprečevanje zanikanja istovetnosti omrežnih transakcij; sledljivost informacij in uporabnikov ter skrbnikov omrežja; zmožnost nadzora nad neavtorizirano uporabo omrežnih virov in zmožnost nadzora nad zlorabo dostopa do omrežja (ISO, 2009, str. 20). Pri tem se standard opira na prakso varovanja informacij, kot jo podajajo standardi ISO/IEC 27001, ISO/IEC 27002 in ISO/IEC 27005. Ta zahteva oceno varnostnih tveganj in vodstveni pregled, na podlagi katerih se identificira in potrdi tehnične in ne-tehnične varnostne kontrole ter predvideno varnostno arhitekturo. Aktivnosti, ki jih standard predpisuje za izpolnitev teh zahtev, so določitev ukrepov za zmanjšanje škodljivega vpliva nepredvidenih incidentov na poslovanje organizacije s stališča pomembnosti informacij in storitev, ki se prenašajo preko omrežja ali so preko omrežja dostopne, identifikacija in ocena verjetnosti uresničitve posameznih groženj, ki vplivajo na informacije in storitve, identifikacija in ocena stopnje kritičnosti izrabe posameznih ranljivosti, ki smo jih identificirali v ocenjenih grožnjah, ocena ukrepov po posameznih tveganjih glede na ukrepe, določene v prvi alineji in identifikacija tehničnih varnostnih ukrepov in področij kontrole, ki bi zaznana tveganja odpravila ali zmanjšala (ISO, 2009, str. 21).

2.2.2.3 Podporne kontrole

V osmem poglavju standard predstavlja pregled podpornih kontrol, ki podpirajo tehnično varnostno arhitekturo omrežja ter ostalih kontrol, ki so poleg varovanja omrežij vezane tudi na

splošno varovanje informacij. Delijo se na osem sklopov, in sicer upravljanje omrežne varnosti, upravljanje tehničnih ranljivosti, identifikacijo in overjanje, zagotavljanje in nadzorovanje revizijskih zapisov, zaznavanje in preprečevanje vdorov, zaščito pred škodljivo kodo, kriptografske storitve in neprekinjeno poslovanje.

a) Upravljanje omrežne varnosti

V tem sklopu standard obravnava kontrole za zagotavljanje varnega upravljanja omrežne varnosti. To mora biti v skladu s politiko varovanja informacij organizacije, kontrole pa so postavljene v štiri sklope, ki obravnavajo problematiko zagotavljanja varnega upravljanja omrežne varnosti, vloge in odgovornosti, nadzorovanje omrežja ter periodično ocenjevanje varnosti omrežja oziroma omrežne varnosti (ISO, 2009, str. 22).

- Aktivnosti upravljanja omrežne varnosti

Da bi organizacija lahko dosegla želeno oziroma zahtevano varnost omrežij, mora skladno z varnostno politiko organizacije izvajati aktivnosti upravljanja omrežne varnosti. Pripraviti mora varnostno politiko omrežja, ki se mora skladati z zahtevami politike varovanja informacij organizacije, njene zahteve pa morajo biti takšne, da jih je mogoče izvesti s tehničnimi ali organizacijskimi prijemi. Politika mora vsebovati stališče organizacije glede sprejemljive rabe omrežij, jasna pravila za varno uporabo omrežnih virov, storitev in aplikacij, specifikacijo posledic neupoštevanja zahtev politike, stališče organizacije glede zlorabe omrežja ter utemeljitve varnostne politike omrežja in specifičnih varnostnih zahtev. Za utemeljitev politike in specifičnih varnostnih zahtev lahko politika vsebuje tudi povzetek ocene varnostnih tveganj in vodstvenega pregleda ter varnostnih kontrol, predpisanih za posamezno tveganje. Poleg politike varovanja omrežij mora organizacija pripraviti tudi operativne postopke, ki se nanašajo na zagotavljanje varnost omrežij v skladu s politiko. Vsi dokumenti morajo določati tudi skrbnika, ki je odgovoren za njihovo uporabo, revidiranje in posodabljanje (ISO, 2009, str. 23-24).

Za zagotavljanje varnosti omrežja organizacije, mora organizacije pripraviti še dva zelo pomembna dokumenta, ki obravnavata oddaljen dostop uporabnikov do omrežja organizacije in povezovanje omrežij različnih organizacij. Dokumenta morata vsebovati natančne zahteve in pogoje, pod katerimi se takšne povezave lahko izvedejo. Pri povezovanju z drugimi organizacijami mora organizacija natančno opredeliti različna tveganja, ki pri tem nastajajo. Standard pri tem opozarja predvsem na zagotavljanje zasebnosti in zaščito osebnih ter komunikacijskih podatkov. Pri določanju teh zahtev mora organizacija upoštevati zakonska določila, paziti pa mora predvsem pri povezovanju z organizacijami v drugih državah, kjer lahko zakonodaja določen tip podatkov obravnava drugače. Dokument mora vsebovati tudi vse varnostne zahteve povezave, obveznosti in odgovornosti vseh organizacij pri zagotavljanju varnosti povezave in zahteve po preverjanju skladnosti z dogovorom. Podobno standard zahteva tudi pri pripravi dokumenta, ki določa varnostne zahteve pri oddaljenem dostopu uporabnikov

do omrežja organizacije. Dokument mora natančno določati obveznosti in odgovornosti uporabnikov glede zagotavljanja strojne in programske opreme, dostopa do podatkov in varnostnih postopkov, ki se jih morajo uporabniki držati (ISO, 2009, str. 24-25).

Ena pomembnejših aktivnosti pri zagotavljanju varnosti omrežja pa je tudi upravljanje incidentov. Standard zahteva vzpostavitev sistema upravljanja incidentov, ki bo zmožen obravnavati različne dogodke, povezane z informacijsko varnostjo in zaznane varnostne incidente. Omogočati mora čim hitrejši odziv ob nastanku incidenta in posledično zmanjšanje njegovega vpliva na delovanje in varnost omrežja ter informacijskih sistemov. Z dokumentiranjem varnostnih incidentov se bo v njem gradila baza znanja, na podlagi katere lahko podobne incidente organizacija prepreči ali se na njih hitreje odzove. Standard za vzpostavitev sistema upravljanja incidentov predlaga pregled priporočil v standardu ISO/IEC 27035 (ISO, 2009, str. 25).

- Vloge in odgovornosti povezane z varovanjem omrežij

V tej točki nam standard (ISO, 2009, str. 25-26) predlaga naslednjo vzpostavitev vlog in pripadajočih odgovornosti:

- Višje vodstvo, katerega naloge so definiranje varnostnih ciljev organizacije; priprava, sprejetje, objava in uveljavljanje varnostne politike organizacije, postopkov, pravil in politike sprejemljive rabe; uveljavljanje varnosti in politike sprejemljive rabe.
- Skupina za upravljanje omrežja, katere naloge so priprava varnostne politike omrežja; izvajanje varnostne politike omrežja in politike sprejemljive rabe; komunikacija z zunanjimi deležniki in zagotavljanje izvajanje obojestranske varnostne politike povezanih omrežij; zagotavljanje, da sta operativna odgovornost za omrežja in računalniške sisteme ločeni.
- Skupina za varnost omrežij, ki mora skrbeti za nabavo, razvoj, testiranje, preverjanje in vzdrževanje komponent in orodij za zagotavljanje omrežne varnosti; vzdrževanje orodij in komponent za zagotavljanje omrežne varnosti s stalnim sledenjem razvoja groženj, kot na primer nadgrajevanje protivirusnih sistemov; posodabljanje nastavitev na sistemih za zagotavljanje omrežne varnosti glede na zahteve in spremembe poslovnih procesov, kot na primer posodabljanje seznamov za kontrolo dostopa.
- Skrbniki omrežij, katerih naloge so nameščanje, nadgrajevanje, uporaba in zaščita storitev in komponent za zagotavljanje omrežne varnosti; izvajanje vsakodnevnih opravil, ki zagotavljajo skladnost z varnostno politiko omrežja; izvajanje ustreznih ukrepov, ki zagotavljajo zaščito varnostnih komponent omrežja, kot na primer preverjanje delovanja omrežja, odzivanje na varnostne incidente, izvajanje varnostnega kopiranja itd.
- Uporabniki omrežij, ki morajo omrežje uporabljati skladno z varnostno politiko in politiko sprejemljive rabe omrežnih virov; sporočati svoje varnostne zahteve, sporočati morebitne incidente in ostale varnostne dogodke povezane z omrežjem, podajati povratne informacije o učinkovitosti omrežne varnosti.
- Revizorji, katerih naloge so periodično revidiranje učinkovitosti omrežne varnosti;

preverjanje skladnosti z varnostno politiko omrežja; preverjanje in testiranje skladnosti operativnih omrežnih varnostnih pravil s poslovnimi zahtevami in zakonskimi omejitvami.

- Presoja omrežne varnosti

Standard v tej točki zahteva periodično preverjanje skladnosti varovanja omrežij s politiko varovanja omrežij. Pri tem je treba preveriti izvajanje vseh kontrol, ki so zapisane v varnostni politiki omrežja, operativnih procedurah, dokumentu tehnične varnostne arhitekture omrežja, varnostni politiki varnih prehodov, načrtu neprekinjenega poslovanja in predpisanih varnostnih zahtev komunikacijskih povezav. Skladnost je treba preverjati pred vzpostavitvijo oziroma začetkom uporabe nove povezave ali omrežja, ob vsaki večji spremembi in seveda tudi v predpisanih intervalih. Ker je omrežna varnost dinamični koncept, standard predlaga sledenje aktualnim spremembam na področju zagotavljanja omrežne varnosti, nameščanje varnostnih popravkov in periodično revizijo obstoječih varnostnih kontrol glede na uveljavljene pristope, kot so varnostna testiranja, preverjanje ranljivosti in penetracijska testiranja v skladu z varnostno politiko in aktualno zakonodajo držav, preko katerih se omrežje organizacije razteza. Poročilo varnostnega testiranja mora vključevati vse varnostne pomanjkljivosti in morebitne ranljivosti, predloge za njihovo odpravo ter prioriteto in predviden datum odprave (ISO, 2009, str. 26).

b) Upravljanje tehničnih ranljivosti

Tehnične ranljivosti imajo lahko velik vpliv na delovanje in varnost omrežij. Organizacija mora najprej izvesti popis komunikacijskih virov in vseh potrebnih značilnosti, kot na primer tip naprave, različica strojne in programske opreme, odgovorni skrbnik naprave, lokacija naprave itd. Na podlagi popisa mora nato zbrati in oceniti podatke o tehničnih ranljivostih za posamezno napravo, oceniti izpostavljenost naprave do določene ranljivosti ter na podlagi teh podatkov določiti, izvesti in preveriti pripadajoče varnostne kontrole, vezane na zaznana tveganja (ISO, 2009, str. 26-27).

c) Identifikacija in overjanje

Standard v tej točki poudarja pomembnost omejevanja dostopov do omrežja in informacijskih virov na avtorizirane uporabnike in izpostavlja avtorizacijo uporabe omrežnih virov. Pri tem so pomembna tri področja kontrole, in sicer oddaljeni dostop, uporaba naprednejših sistemov overjanja in uporaba varnega enkratnega vpisa. Pri oddaljenem dostopu do omrežja in omrežnih virov organizacije je treba poskrbeti za identifikacijo in overjanje uporabnikov ter omejevanje dostopov v skladu z varnostno politiko. Standard predlaga, da oddaljenim uporabnikom organizacija dovoli dostop do omrežij, ki zahtevajo višji nivo varnosti, le ob zagotavljanju dodatnih varnostnih mehanizmov, kot je na primer šifriranje povezave. Naslednje področje kontrole je uporaba naprednejših sistemov overjanja, kot sta identifikacija kličočega in overjanje uporabnikov z digitalnimi potrdili, shranjenimi na pametnih karticah in zaščitenimi z

osebnimi številkami ali biometričnimi zapisi. Zadnje področje kontrole pa se nanaša na uporabo varnega enkratnega vpisa v primerih, ko različni sistemi od uporabnika zahtevajo večkratni vpis poverilnic. Sistem varnega enkratnega vpisa dovoli uporabniku po prvem vpisu poverilnic dostop do vseh informacijskih virov, ki jih potrebuje za upravljanje svojega dela, standard pa za prvi vpis predlaga uporabo naprednih sistemov overjanja (ISO, 2009, str. 27).

d) Zagotavljanje in spremljanje revizijskih zapisov

V tej točki se standard navezuje na kontrole, ki jih predvidevata standarda ISO/IES 27002 in ISO/IEC 27005. Zahteva vzpostavitev varnega centralnega sistema za hranjenje revizijskih zapisov za potrebe nadzora, revizij in raznih analiz. Ta sistem mora hraniti podatke o napačnih prijavah v sisteme, napačnih ponovnih prijavah, kršitvah dostopov preko varnih prehodov, poskuse oddaljenih dostopov do revizijskih zapisov ter opozorila in alarme, ki jih ustvarijo sistemi ob varnostnih incidentih, kot na primer podvojena uporaba internetnih naslovov, izpadi povezav itd. Zapisi morajo vsebovati tudi natančno uro in datum dogodka ter izvorni sistem, zbirati pa se morajo iz vseh sistemov, ki sestavljajo omrežje organizacije. Varni centralni strežnik mora omogočati analizo zapisov, prikaz dogodkov v realnem času, zaščito pred nepooblaščenim dostopom, sledljivost dostopov, dolgoročno hrambo in iskanje zapisov ter pripravo poročil na nivoju uporabnikov, aplikacij in tipa informacij glede na specificirane časovne omejitve. Čas hrambe zapisov oziroma revizijskih sledi mora biti usklajen s politiko varovanja informacij in aktualno zakonodajo, revizijske sledi pa je treba do poteka hrambe varno hraniti v sistemih ali na medijih, ki omogočajo enkratno pisanje in večkratno branje. Vzpostavitev takega sistema je pomembna za dokazovanje istovetnosti zapisov v primerih, ko je treba dokazovati prenos podatkov preko omrežja organizacije in ob različnih varnostnih incidentih. Organizacija mora zagotoviti tudi stalno spremljanje revizijskih zapisov, alarmov in opozoril, ki jih ustvarijo različne naprave v omrežju, poročil varnostnih pregledov omrežij in pregledov skladnosti z varnostnimi zahtevami ter ne nazadnje tudi vseh varnostnih dogodkov in incidentov, ki so jih javili uporabniki ali podporno osebje (ISO, 2009, str. 28-29).

e) Zaznavanje in preprečevanje vdorov

V tej točki standard zahteva vzpostavitev sistemov za zaznavanje in preprečevanje vdorov. Sistemi morajo omogočati zaznavanje in preprečevanje vdorov, obveščanje odgovornega osebje o vsakem zaznanem poskusu vdora, zagotavljati revizijsko sled vdora na način, ki omogoča organizaciji analizo vdora ter vzorčenje delovanja informacijskega sistema (ISO, 2009, str. 29).

f) Zaščita pred škodljivo kodo

Škodljiva koda se večinoma širi preko javnih in zasebnih omrežij, zato je treba vzpostaviti primerne varnostne kontrole, ki bodo zaščitile informacijsko infrastrukturo organizacije pred škodljivo kodo. Standard pri tem predvideva uporabo namenske programske opreme za ščitenje pred škodljivo kodo, ki jo je treba namestiti na strežnike, delovne postaje znotraj organizacije,

delovne postaje in prenosne sisteme uporabnikov oddaljenega dostopa, ter na požarne pregrade, če to omogočajo. Tako programsko opremo kot baze podpisov škodljive kode je treba redno nadgrajevati. Ker tovrstni sistemi niso popolnoma zanesljivi, in ker se z dostopom do zunanjih omrežij povečuje tudi tveganje okužbe, standard kot učinkovito preprečevanje širjenja škodljive kode predlaga tudi izklop vseh nepotrebnih storitev in funkcij na vseh napravah, ki so priključene na omrežje organizacije (ISO, 2009, str. 29-30).

g) Kriptografske metode in storitve

V primeru potreb po zagotavljanju zaupnosti in preprečevanju zanikanja istovetnosti, uporabi oddaljenega nastavljanja omrežnih naprav ter prenašanju revizijskih sledi standard zahteva uporabo kriptografskih kontrol. V primerih, ko je treba dokazovati izvedbo prenosa informacij preko omrežja, predlaga uporabo komunikacijskih protokolov, ki omogočajo potrdilo o oddaji oziroma predložitvi, aplikacijske protokole, ki zahtevajo naslov ali enolični identifikator pošiljatelja, prehode, ki omogočajo preverjanje naslovov pošiljatelja in prejemnika glede na sintakso in preverjanjem v relevantnih imenikih, protokole, ki omogočajo potrditev prejema informacij in zagotavljajo ugotavljanje zaporedja dogodkov.

V procesih, ki zahtevajo zagotavljanje istovetnosti pošiljatelja in zaupnosti poslanih podatkov, standard zahteva uporabo digitalnih podpisov in šifrirnih algoritmov v skladu z zahtevami varnostne politike in veljavne zakonodaje. (ISO, 2009, str. 30-31).

h) Neprekinjeno poslovanje

V tej točki standard zahteva vzpostavitev vseh potrebnih kontrol za zagotavljanje neprekinjenega poslovanja v primerih katastrof. Organizacija mora pripraviti strategijo neprekinjenega poslovanja, ki mora določati vse pomembne poslovne procese in načrte izvajanja procesov ponovne vzpostavitve kritične infrastrukture v primeru katastrofe. S stališča omrežja je treba v takšnih primerih zagotoviti vse povezave in omrežja, ki jih organizacija potrebuje za vzpostavitev najbolj kritičnih poslovnih procesov. To vključuje vzpostavitev redundantnih povezav z minimalno zahtevano kapaciteto in načrte ponovne vzpostavitve vseh povezav v primeru neželenih dogodkov (ISO, 2009, str. 31-32).

2.2.2.4 Smernice za snovanje in izvedbo omrežne varnosti

Smernice za snovanje in izvedbo omrežne varnosti so v prvem delu standarda le okvirno zapisane, detajlno pa jih pokriva drugi del standarda, ISO/IEC 27033-2, ki je v tem magistrskem delu prestavljen v točki 2.3.

2.2.2.5 Referenčna omrežja - tveganja, tehnike načrtovanja in problemi nadzora

Tveganja, tehnike načrtovanja in problemi nadzora v referenčnih omrežjih so v prvem delu

standarda le okvirno zapisani, detajlno pa jih pokriva tretji del standarda, ISO/IEC 27033-3, ki je v tem magistrskem delu prestavljen v točki 2.4.

2.2.2.6 Tehnološke teme – tveganja, tehnike načrtovanja in problemi nadzora

V tej točki se standard sklicuje na prilogo A, ki je zgolj informativne narave. Ker vse točke priloge obravnavajo tudi drugi deli standarda, priloge v magistrskem delu ne bom obravnaval.

2.2.2.7 Razvoj in testiranje varnostne rešitve

Dokumenti, narejeni v predhodnih točkah, sestavljajo tehnično varnostno arhitekturo podjetja. Ko je pripravljena in odobrena s strani vodstva jo je treba razviti, pripraviti testno okolje in z natančnim testiranjem preveriti njeno skladnost z vsemi zahtevami. To poteka v dveh korakih. V prvem koraku mora organizacija s testiranjem potrdili primernost rešitve. Za izvedbo testiranja je treba pripraviti strategijo testiranja, pristop k testiranju in načrt testiranja. Slednji mora biti usklajen tudi z vsemi morebitnimi nacionalnimi, vladnimi in lokalnimi standardi vseh držav, preko katerih se omrežje organizacije širi. V tem koraku je treba izvesti tudi penetracijsko testiranje, s katerim se potrdi varnost testnega okolja. Ko je rešitev v prvem koraku potrjena, je treba preveriti njeno skladnost s tehnično varnostno arhitekturo, varnostno politiko omrežja, predvidenim sistemom upravljanja varovanja omrežij, varnostno politiko varnih prehodov, načrtom neprekinjenega poslovanja in varnostnimi zahtevami povezav. Poročilo o skladnosti mora vsebovati zapise o neuspelih testih, zaznanih neskladnostih in posledičnih spremembah varnostne rešitve ter prioriteto in čas za odpravo odkritih napak in neskladnosti. Dokumente, ki nastanejo v teh procesih, mora pred začetkom uporabe rešitve potrditi tudi višje vodstvo organizacije (ISO, 2009, str. 37-38).

2.2.2.8 Upravljanje varnostne rešitve

Vsakodnevno upravljanje varnostnih rešitev zahteva stalni nadzor in revidiranje, ob vsaki večji spremembi pa je treba ponovno izvesti testiranje in preverjanje skladnosti, kot jih opisuje prejšnja točka (ISO, 2009, str. 38).

2.2.2.9 Nadzorovanje in revidiranje izvedba rešitve

Standard v tej točki zahteva stalni nadzor in preverjanje skladnosti, kot je to opisano v točki 2.2.2.7. S tem povezane aktivnosti je treba izvajati periodično, ob vsaki večji spremembi in izvedbi novih varnostnih rešitev (ISO, 2009, str. 38).

2.3 ISO/IEC 27033-2:2012

Drugi del standarda, ISO/IEC 27033-2, ima naziv Smernice za zasnovo in izvedbo varovanja omrežij in je bil izdan leta 2012. Podaja smernice, kako načrtovati, snovati, izvesti in

dokumentirati omrežno varnost (ISO, 2012, str. 1).

2.3.1 Obseg in struktura

Drugi del standarda podaja priporočila in zahteve za pripravo informacij, ki so potrebne za snovanje omrežne varnosti, smernice za snovanje omrežne varnosti in korake izvedbe. Izvedbo predlaga v treh fazah. V prvi fazi mora organizacija prepoznati vse potrebne vire in pripraviti nabor zahtev, ki jih določajo različni zakoni, regulatorji, poslovni procesi ter zahteve po minimalni zmogljivosti omrežja. Te informacije so ključnega pomena za uspešno izvedbo druge faze, kjer standard predstavi različne principe snovanja omrežne varnosti, kot so poglobljen pristop k varovanju omrežij, razmejevanje varnostnih območij, odpornost omrežja na različne grožnje ter predstavi modele in ogrodja snovanja varnih omreži. Zadnja faza je namenjena izvedbi omrežne varnosti, kjer standard predstavi merila za izbor omrežnih komponent, produktov in proizvajalcev, zahteve pri upravljanju omrežja, nadzoru omrežja in odzivanju na incidente ter dokumentiranje, načrtovanje testiranja in izvedbo testiranja omrežne varnostne arhitekture. Ta del standarda vsebuje tudi tri priloge. Priloga A podaja reference med poglavji ISO/IEC 27033-2:1012 s poglavji standardov ISO/IEC 27001:2005 in ISO/IEC 27002:2005. Priloga B podaja predloge dokumentov, ki jih ta del standarda zahteva, priloga C pa predstavlja ITU-T X.805 ogrodje in preslikavo kontrol s standardom ISO/IEC 27001:2005 (ISO, 2012).

2.3.2 Priporočila in zahteve

2.3.2.1 Priprava na snovanje omrežne varnosti

Priprava na snovanje omrežne varnosti je proces zbiranja informacij ter revizija možnosti, omejitev, zasnove in izvedbe obstoječega omrežja. V prvi fazi standard zahteva identifikacijo vseh sredstev, ki vplivajo na izvajanje poslovnih procesov in morajo biti primerno zaščitena. Sredstva deli na fizična, kot so na primer strežniki, omrežna stikala, usmerjevalniki, vmesniki, protokoli itd., in logična, kot so nastavitve naprav, izvršljiva koda, podatki, informacije itd. Omrežno varnost torej sestavlja varovanje omrežne infrastrukture, poslovnih procesov in z njimi povezanih informacij. Pri identifikaciji sredstev standard predlaga tri vprašanja: katere specifične tipe omrežne opreme, skupine objektov, informacijska sredstva in zmogljivosti procesiranja je treba varovati, katere specifične tipe omrežnih aktivnosti je treba varovati in katera informacijska sredstva so v arhitekturi informacijskega sistema (ISO, 2012, str. 3).

V naslednji fazi je treba pripraviti evidenco vseh zahtev, ki vplivajo na zasnovo omrežja. To so zakonske in regulatorne zahteve, poslovne zahteve in zahteve glede zmogljivosti omrežja. Pri zbiranju in pregledu zakonskih in regulatornih zahtev, ki vplivajo bodisi na lokacijo bodisi na funkcijo omrežja, je treba posebno pozornost nameniti omrežjem, ki se raztezajo preko več držav. V takšnih primerih je treba zbrati zahteve vseh držav, preko katerih se razprostira omrežje in skladno z zahtevami prilagoditi njegovo zasnovo. Naslednji korak je zbiranje poslovnih zahtev. Poslovne zahteve se nanašajo na zahteve po dostopu do podatkov. Omrežje

mora omogočati varen dostop do zahtevanih podatkov le avtoriziranim uporabnikom in sistemom. Evidenca mora vsebovati sisteme, njihova polna domenska imena, IP naslove, MAC naslove in za vsako storitev tudi protokolna vrata storitve. Za zagotavljanje nemotenega delovanja vseh storitev in dostopov standard zahteva še zbiranje podatkov o prometu, propustnosti obstoječih povezav in omrežja ter zmogljivosti aktivne omrežne opreme. Določiti je treba najmanjše, povprečno in največje število hkratnih uporabnikov na posamezni povezavi ali delu omrežja, maksimalno število hkratnih povezav na spletne in podatkovne strežnike ter predvideti rast teh zahtev za obdobje petih let. Zbrane podatke je treba analizirati in določiti optimalno propustnost posameznih povezav in omrežij, ki bo zagotavljala nemoteno delo vsem uporabnikom v mejah razumnih stroškov (ISO, 2012, str. 3-4).

Ko so vse predhodno naštete informacije zbrane, je treba izvesti revizijo vseh zbranih zahtev, katere cilj je potrditev skladnosti obstoječe in načrtovane tehnične arhitekture z vsemi prepoznanimi zahtevami. Izhodni dokument te faze mora vsebovati opredelitev tipov omrežnih povezav, evidenco varnostnih tveganj, evidenco zahtevanih varnostnih kontrol, tehnično varnostno arhitekturo, evidenco predvidenih omrežnih protokolov ter popis omrežnih aplikacij po posameznem nivoju omrežja. Če predvidena arhitektura ne omogoča izvedbe vseh varnostnih kontrol, jo moramo v skladu z zahtevami popraviti in nato ponovno revidirati vse zahteve. Zahteve, ki jih ni mogoče izpolniti, je treba zabeležiti, predvideti kontrole, s katerimi je mogoče preostala tveganja zmanjšati ter ponovno oceniti (ISO, 2012, str. 4).

Zadnji korak priprave na snovanje omrežne varnosti je še analiza odstopanj med analizo tveganj obstoječe varnostne arhitekture ter predvidenih varnostnih kontrol. Morebitna odstopanja je treba analizirati, pripraviti nove varnostne kontrole in jih vključiti v novo varnostno arhitekturo omrežja (ISO, 2012, str. 5).

2.3.2.2 Snovanje omrežne varnosti

V tem poglavju standard predstavlja proces in principe snovanja omrežne varnosti. Cilj poglavja je priprava omrežne varnostne arhitekture, katere namen je omejevanje prenosa podatkov med različno varnimi omrežji. Končni dokument mora vsebovati evidenco vseh povezav med omrežji, predvidene varnostne kontrole za posamezno povezavo ter vse tehnične predpostavke, kot na primer izbor komunikacijskega protokola ter zahteve po tuneliranju ostalih protokolov. Standard za zagotavljanje varne omrežne infrastrukture določa tudi minimalni nabor varnostnih storitev. Te so identifikacija in overjanje uporabnikov in naprav z uporabo različnih metod, kot so uporabniška imena in gesla, digitalna potrdila, avtorizacija ukazov itd.; logična kontrola dostopov, kot na primer sistemi varnega enkratnega vpisa, kontrole dostopov glede na vlogo uporabnika, kontrola aplikacij, požarne pregrade, posredniški strežniki (angl. *proxy server*) itd.; varnostna presoja in obračunski zapisi, pod kar spadajo zapisi za presojo, sistemi in storitve za analizo zapisov za presojo, sistemi za zaznavanje vdorov, sistemi, ki omogočajo enkratno zapisovanje ter večkratno branje itd.; sistemi za zagotavljanje varnega brisanja in uničenja podatkov; varnostno testiranje, ki vključuje preverjanje ranljivosti na

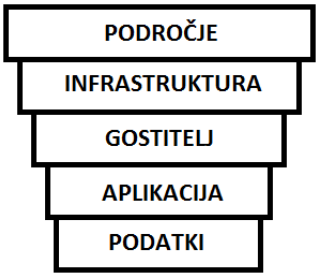
sistemih, vohljanje za paketi na omrežju, penetracijsko testiranje itd.; segregacija testnih, razvojnih in produkcijskih okolij; upravljanje s spremembami; sistem za distribucijo programske opreme z uporabo varnih protokolov, kot na primer digitalno podpisovanje, uporabljanje protokolov za zagotavljanje varne komunikacije, kot na primer TLS itd.; varno upravljanje in zagotavljanje visoke razpoložljivosti z uporabo dobrih sistemov za izvajanje in obnavljanje varnostnih kopij, odpornost na izpade, uporaba tehnologije gruč itd.; uporaba šifriranja prenosa podatkov, tehnologije razpršenega spektra, navideznih zasebnih omrežij itd.

Glavni principi snovanja, ki jih standard v tej točki predvideva, so poglobljena obramba, uporabo omrežnih področij, odpornost zasnove, uporaba referenčnih omrežij pri snovanju omrežne varnostne infrastrukture in uporaba varnostnih okvirjev (ISO, 2012, str. 5-6).

a) Poglobljena oziroma večslojna obramba

Poglobljeno oziroma večslojno obrambo sestavljajo varnostna politika, zasnova, upravljanje in tehnologija. Vsaka od naštetih komponent vsebuje svoje varnostne kontrole in tehnike, s katerimi pripomore k zmanjšanju tveganja v primeru odpovedi ali zaobidenja druge komponente. Kot primer večslojnih tehničnih varoval podaja standard uporabo protivirusnega programa na požarnih pregradah, strežnikih in delovnih postajah hkrati ter uporabo protivirusnih programov različnih proizvajalcev. Drug primer večslojnih tehničnih varoval je varovanje brezžičnih dostopov, pri čemer standard predlaga povezovanje brezžičnih dostopnih točk v demilitarizirana področja, uporabo varnostnega standarda WPA in filtriranje MAC naslovov. Kot primer uporabe več komponent varnosti hkrati, pa standard podaja nevarnost uporabe mobilnih naprav, ki navadno omogočajo povezovanje z drugimi napravami preko USB priključka, povezovanje preko različnih brezžičnih omrežij in mobilno povezovanje z internetom. S tako napravo je enostavno zaobiti tehnične varnostne kontrole na omrežju in delovno postajo povezati neposredno z internetom. To je treba preprečiti z varnostno politiko in tehničnimi varnostnimi kontrolami, kot je na primer preprečevanje uporabe USB naprav ter rutinsko pregledovanje brezžičnih frekvenc z namenom zaznave nedovoljenih dostopnih točk. Namen vseh slojev je, da ščitijo podatke in vsak sloj robu našega omrežja do podatkov definira bolj natančne varnostne kontrole za varovanje podatkov (ISO, 2012, str. 6-7). Grafični prikaz poglobljene obrambe po standardu prikazuje slika 2.

Slika 2: Pristop k poglobljeni obrambi



Vir: ISO, ISO/IEC 27033-2:2012, 2012, str.7.

b) Uporaba omrežnih področij

Omrežna področja so namenjena ločevanju sistemov z različnimi varnostnimi zahtevami oziroma različno toleranco do tveganj. Ta se lahko nanaša na občutljivost podatkov ali na izpostavljenost zunanjim omrežjem organizacije, kot na primer internetu. Promet znotraj nekega omrežnega področja lahko med sistemi potuje brez omejitev, promet v ali iz področja pa mora biti strogo nadzorovan z varnostnimi prehodi, kot so požarne pregrade, sistemi za zaznavanje in preprečevanje vdorov ter usmerjevalniki ali stikala, ki imajo nameščene sezname za kontrolo dostopov. Standard na tem mestu predpisuje pravila snovanja po t. i. principu kompartmentalizacije. To pomeni, da morajo biti omrežja z različnimi varnostnimi zahtevami ločena in postavljena v različna varnostna področja. Pri ločevanju mora organizacija poskrbeti, da so vse naprave in sistemi, katerih storitve so in morajo biti dosegljive uporabnikom omrežij zunaj organizacije, nameščeni v posebno področje, ločeno od notranjih sistemov, da morajo biti strateška sredstva nameščena v ločenem namenskem varnostnem področju in, da morajo biti vse naprave in sistemi nižjega zaupanja nameščeni v ločenem varnostnem področju. V različna varnostna področja je treba postaviti tudi omrežja različnih tipov, torej omrežja strežnikov in omrežja uporabnikov, sisteme za upravljanje omrežja in varnosti ter ločiti razvojne in produkcijske sisteme (ISO, 2012, str. 7).

c) Odpornost zasnove omrežja

Kot je bilo omenjeno že v točki priprave na snovanje omrežne varnosti, je treba za nemoteno delovanje omrežja predvideti več slojev redundance z namenom odprave kritične točke odpovedi omrežja. V skladu z večslojnim pristopom moramo tudi tu k cilju pristopiti na različne načine, z vzpostavitvijo redundantnih povezav, podvojenih modulov, naprav v stanju pripravljenosti in topologije, ki omogoča redundantne poti. Pri zagotavljanju varnosti je treba uporabljati različne funkcionalnosti, ki se med seboj dopolnjujejo in v neki meri tudi prekrivajo (ISO, 2012, str. 7).

d) Scenariji referenčnih omrežij

V tej točki standard predlaga primerjavo pripravljene zasnove omrežja z referenčnimi omrežji. V tretjem delu standarda, ISO/IEC 27033-3, so predstavljena različna omrežja s predvidenimi tveganji, varnostnimi tehnikami in kontrolami, obravnavane pa so tudi različne zasnove za posamezni scenarij omrežja (ISO, 2012, str. 8).

e) Modeli in okvirji

Poleg uporabe referenčnih omrežij, standard predlaga tudi uporabo že razvitih varnostnih modelov in okvirjev. Varnostni okvirji predstavljajo priporočila za zagotavljanje omrežne varnosti na celotni poti in načine formiranja splošne varnostne strukture, varnostni modeli pa se osredotočajo na zaupnost in celovitost omrežij in informacijske infrastrukture. Z njimi si lahko

pomagamo pri definiranju dostopnih pravil v skladu z varnostno politiko. Kot primer varnostnega okvirna standard opisuje ITU-T X.805, ki je podan kot priloga drugemu delu standarda (ISO, 2012, str. 8).

V zadnji točki snovanja omrežne varnosti standard zahteva, da predlog varnostne zasnove omrežja odobri ustrezen nivo vodstva (ISO, 2012, str. 8).

2.3.2.3 Izvedba

Po končani pripravi in odobritvi varnostne zasnove omrežja je treba zasnovano omrežno varnost še izvesti. Pri tem standard opisuje sedem pomembnih gradnikov izgradnje oziroma izvedbe omrežne varnosti.

Prvi gradnik so merila za izbiro omrežnih komponent, s katerimi gradimo tehnično varovanje omrežja in morajo zadovoljiti vse zahteve, ki so bile zapisane v prejšnjih točkah in poglavjih. Ključne komponente so segmentacija in kompartmentalizacija, sistemi za upravljanje varnosti, osnovne varnostne tehnologije, naprave za krmiljenje dostopov, tehnike za zmanjševanje groženj, naprave na obrobju omrežij, naprave za omejevanje omrežnih dostopov, sistemi za zaznavanje in preprečevanje vdorov, zaščita končne točke, usmerjevalniki in stikala ter povezave omrežji različnih organizacij (ISO, 2012, str. 9).

Drugi gradnik so merila za izbiro proizvodov in dobaviteljev. Merila za izbiro proizvoda morajo temeljiti na tehnični primernosti in prednostih proizvoda, zmogljivosti, združljivosti, odpornosti na izpade in razširljivosti proizvoda. Proizvod mora podpirati vse zahtevane protokole, omogočati revizijsko sled in skladnost s predpisi ter imeti vso potrebno dokumentacijo, procedure vzdrževanja in diagnostike napak ter vsebovati logično varnostno strukturo (ISO, 2012, str. 9). Pri izbiri dobavitelja je treba analizirati sposobnost izvedbe naročila, kakovost, velikost, bilanco uspehov, položaj na trgu, finančno stabilnost, možnost izobraževanja, reference in kompetence pri prodaji ter integraciji tovrstnih produktov, čas dobave in tudi stroške (ISO, 2012, str. 10).

Tretji gradnik se nanaša na postopke upravljanja omrežja v fazi končane izvedbe. Standard definira upravljanje omrežja kot aktivnosti, metode, procedure in orodja, ki se nanašajo na skrb za obratovanje, administracijo, vzdrževanje in oskrbo sistemov, ki sestavljajo omrežje organizacije. Skrb za obratovanje omrežja se navezuje na nadzorovanje omrežja, velik del tega pa je zaznavanje in odpravljanje napak v najkrajšem možnem času ter ohranjanje omrežja v delujočem stanju. Administracija omrežja se navezuje na skrbno dodeljevanje in spremljanje omrežnih virov, vzdrževanje pa na izvajanje nadgradenj, popravil in nameščanje (nove) omrežne opreme. V sklopu upravljanja omrežja je treba skrbeti za varnostne kontrole, ki preprečujejo namerno ali nenamerno napačno nastavitev omrežne opreme, saj to lahko vplivala na delovanje omrežja in zagotavljanje celovitosti ter zaupanja. Standard te kontrole deli na organizacijske in tehnične. Organizacijske kontrole vključujejo razmejevanje pravic skrbnikov

omrežne opreme, deljenje pooblastil, uveljavljanje principov za zagotavljanje visokega nivoja varnosti, kot na primer principa štirih oči ter procedure in politike, ki preprečujejo uporabo privzetih in šibkih gesel. Tehnične kontrole se navezujejo predvsem na način dostopa do vseh vmesnikov za upravljanje omrežne opreme. Zagotavljati morajo dovolj visoko stopnjo varnosti z uporabo varnih metod overjanja in avtorizacije skrbnikov in uporabnikov. Oddaljeno upravljanje se mora vedno izvajati s centralne delovne postaje, ki je namenjena zgolj upravljanju omrežnih sistemov in mora omogočati šifriranje komunikacije do omrežnih sistemov ter uporabo naprednega sistema overjanja. Če sistemi ne podpirajo varnih metod dostopa in prenosa podatkov, je varnost treba zagotoviti z uporabo šifriranih tunelov ali navideznih zasebnih omrežij. Enako standard zahteva tudi za uporabo protokolov za nadzor delovanja omrežne opreme (ISO, 2012, str. 10-11).

Beleženje dogodkov na omrežju je eden ključnih gradnikov varnega omrežja, saj omogoča nadzor nad omrežjem in hiter odziv na incidente, ki jih zaznajo posamezne naprave v omrežju. V tej točki standard zahteva vzpostavitev varnega revizijskega strežnika v demilitariziranem področju, ki je ločeno od ostalih omrežij. Omrežje in vse komponente tega omrežja morajo biti dostopni le avtoriziranim osebam. Zapisi iz posameznih komponent omrežja se morajo na revizijski strežnik prenašati z uporabno varnih protokolov, ki zagotavljajo integriteto, celovitost in preprečevanje zanikanja istovetnosti. Anomalije in incidente na omrežju je treba stalno nadzorovati in vzpostaviti sistem alarmiranja, ki ob pojavu posebnega dogodka odgovorne osebe o tem obvesti preko elektronske pošte in/ali SMS sporočil. Odgovorne osebe morajo po prejemu obvestila o incidentu glede na prioriteto oziroma stopnjo alarma sprožiti predpisan postopek analize in reševanje incidenta (ISO, 2012, str. 11).

Končano izvedbo je treba potrditi s testiranjem. Pred začetkom uporabe je treba preveriti, ali tehnična varnostna infrastruktura zadovoljuje vse zahteve in pripraviti dokument strategije varnostnega testiranja. Ta mora vsebovati načrt testiranja tehničnih varnostnih kontrol in zahteve za potrditev njihove skladnosti z vsemi zahtevami varnostne politike. Na podlagi pripravljene strategije je treba pripraviti še načrt testiranja in izvesti vse predvidene teste. Načrt testiranja mora predpisovati tudi podatke, s katerimi bodo testi izvedeni in scenarije testiranja, ki bodo potrdili predpisano funkcionalnost vsake komponente in naprave (ISO, 2012, str. 11-12).

2.4 ISO/IEC 27033-3:2010

Tretji del standarda, ISO/IEC27033-3:2010, nosi naziv Primeri referenčnih omrežij – grožnje, tehnike snovanja in težave nadzora. Izdan je bil konec leta 2010, njegov namen pa je predstaviti scenarije uporabe različnih omrežij in za vsakega od scenarijev predstaviti varnostne grožnje ter smernice za zmanjšanje teh tveganj (ISO, 2010, str. 10).

2.4.1 Obseg in struktura

Standard v tem delu podaja devet scenarijev uporabe referenčnih omrežij, z njimi povezanih varnostnih groženj, tehnik snovanja in kontrol, ki so potrebne za zmanjšanje z grožnjami povezanih tveganj. Služi kot podpora drugemu dela standarda, predvsem v fazi revizije načrtovane tehnične varnostne arhitekture in zasnove. S pomočjo podanih referenčnih omrežij in predvidenih varnostnih tveganj omogoča potrditev, da dokument tehnične varnostne arhitekture predvideva vse grožnje in z njimi povezane varnostne kontrole (ISO, 2010, str. 10).

V uvodnem poglavju standard opiše pristop k obravnavanju varnosti v posameznem referenčnem omrežju. Pogoj za začetek ocenjevanja omrežne varnosti je identifikacija in kategorizacija sredstev, ki jih je treba varovati. Standard predpisuje le grobo kategorizacijo sredstev na infrastrukturna sredstva, storitve in aplikacije, detajlnejša, če je potrebna, pa je prepuščena organizaciji. Pri kategorizaciji je treba paziti na različne vplive ene vrste tveganj na različne kategorije sredstev ter na izpostavljenost aktivnosti različnim tveganjem, kot na primer neavtorizirani spremembi nastavitev preko vmesnika naprave ali s pošiljanjem ukazov preko omrežja. Eno tveganje torej zahteva minimalno dve različni varnostni kontroli (ISO, 2010, str. 4).

Preostalih devet poglavij predstavlja scenarije uporabe različnih referenčnih omrežij. Za vsako podano referenčno omrežje so predstavljeni obseg in namen omrežja, varnostne grožnje, ki se nanašajo na podano omrežje in tabela s tveganji, pripadajočimi varnostnimi kontrolami za zmanjšanje tveganj ter priporočili za snovanje omrežne varnostne arhitekture in tehnologije, ki nam to omogočata. Za identifikacijo tveganj standard priporoča uporabo konsistentne metodologije in sistematičnega pristopa k ocenjevanju, saj le tako lahko podamo primerljive ocene glede na hitro spreminjanje tehnologij. V pomoč pri ocenjevanju tveganj je tudi informativni katalog znanih tveganj, ki je podan kot priloga standarda. Na podlagi ocenjenih tveganj je treba pripraviti protiukrepe in varnostne kontrole, ki vpliv tveganj zmanjšajo (ISO, 2010, str. 4-5). Standard (ISO, 2010, str. 5-6) tu predlaga spisek in definicije varnostnih lastnosti, na katerih so grajeni protiukrepi:

a) Zaupnost se nanaša na zaščito podatkov pred nepooblaščenim razkritjem.
b) Celovitost se nanaša na zaščito podatkov pred nepooblaščenim ustvarjanjem, spreminjanjem, brisanjem in podvajanjem podatkov. Gre torej za ohranjanje pravilnosti in točnosti podatkov.
c) Razpoložljivost se nanaša na zagotavljanje nemotenega dostopa do omrežnih elementov, shranjenih podatkov, pretoka informacij, storitev in aplikacij vsem pooblaščenim uporabnikom ali sistemom.
d) Kontrola dostopa z overjanjem in avtorizacijo uporabnikov in sistemov preprečuje nepooblaščen dostop do omrežnih naprav, omrežnih elementov, shranjenih podatkov, pretoka informacij, storitev in aplikacij.
e) Overjanje je potrjevanje ali dokazovanje identitete uporabnika ali sistema v fazi avtorizacije. Sistem za overjanje mora tudi preprečiti maskiranje enega uporabnika v drugega ter

neavtorizirano ponavljanje dela ali celotne komunikacije.

f) Varne komunikacije in transport podatkov zagotavljajo varen prenos podatkov med avtoriziranimi končnimi točkami komunikacije in preprečujejo prestrezanje ali preusmeritev podatkovnega toka.
g) Preprečevanje zanikanja istovetnosti pomeni zagotavljanje revizijske sledi, s katero poskrbimo, da izvor podatkov ali vzrok nekega dogodka ne moreta biti zanikana.
h) Zakrivanje (angl. *opacity*) zagotavlja zaščito informacij, ki jih je moč izluščiti z opazovanjem omrežnih aktivnosti, kot na primer točko izvora in točko ponora.

V naslednji točki bom predstavil posamezno referenčno omrežje, grožnje in priporočila standarda za zmanjšanje tveganj.

2.4.2 Referenčna omrežja, grožnje in priporočila

Opisana referenčna omrežja predstavljajo scenarije omrežij, s katerimi se navadno srečamo v različnih organizacijah. Priporočila, vezana na prepoznane grožnje pri posameznem referenčnem omrežju, se nanašajo na izvedbo varnostnih kontrol na omrežnem nivoju in so razširitev kontrol za zagotavljanje poslovnih ciljev, ki jih določa standard ISO/IEC 27002 (ISO, 2010, str. 6).

2.4.2.1 Storitve dostopa do interneta za zaposlene

V tej točki je predstavljen scenarij, ki ga srečamo v večini sodobnih organizacij. Zaposleni za izvajanje nalog in doseganje ciljev potrebujejo dostop do interneta, organizacija pa mora pri tem zagotoviti, da zaposleni dostop uporabljajo zgolj za jasno določene in avtorizirane namene. Onemogočiti je treba zlorabo dostopa in s tem povezane grožnje, kot na primer preobremenitev internetne povezave in posledična nedostopnost virov organizacije ali celo pravna odgovornost v primeru zakonske zlorabe dostopa. Organizacija mora za te namene vzpostaviti, nadzorovati in uveljavljati politiko uporabe interneta. Ta mora jasno definirati, da je uporaba interneta dovoljena zgolj v poslovne namene oziroma, če je dostop do interneta dovoljen tudi za zasebne namene, natančne pogoje uporabe in storitve, ki jih je dovoljeno uporabljati. Politika mora določati, ali je dovoljeno uporabljati storitve za napredno sodelovanje, ter ali je zaposlenim dovoljeno sodelovati v raznih forumih, klepetalnicah in podobnih internetnih storitvah (ISO, 2010, str. 6-7).

Politika uporabe interneta je lahko dokaj učinkovit sistem preprečevanja nedovoljene uporabe interneta, a ker so organizacije pri rabi interneta kljub temu še vedno izpostavljene različnim tveganjem, standard opisuje sledeče grožnje in priporočila za njihovo zmanjšanje:

a) Virusi in škodljiva programska koda

Uporabniki interneta so stalno izpostavljeni grožnjam okužbe delovne postaje z virusi ali

škodljivo programsko opremo, kar lahko pripelje do uhajanja informacij, poškodovanja ali namernega spreminjanja podatkov, izpada informacijske infrastrukture in podobno. Večina okužb se zgodi pri prenosu datotek z zlonamerno programsko kodo ali z izrabo ranljivosti v spletnih brskalnikih in spletnih aplikacijah. Možnosti za vnos virusov, zlonamerne programske opreme in trojanskih konjev je največ v okoljih, kjer lahko uporabniki dostopajo do interneta brez vseh omejitev in pri tem uporabljajo aplikacije, ki omogočajo prenos in souporabo datotek. Varnostni mehanizmi, ki jih standard pri tem predlaga, so celovitost, kontrola dostopa in overjanje. Organizacija mora uporabnikom omejiti dostop do interneta s preprečevanjem uporabe in dostopa do nedovoljenih storitev in internetnih aplikacij. Vse datoteke, ki jih uporabniki prenesejo iz interneta, je treba med prenosom preko varnega prehoda, med prenosom na končni sistem ter pri shranjevanju in zaganjanju pregledovati s protivirusnimi programi. Pri dostopu do interneta je treba tudi preprečiti prikaz pojavnih oken in spletnega oglaševanja, ves promet med uporabnikom in internetom pa je vedno treba posredovati preko varnih prehodov, ki omogočajo preverjanje pristnosti vsebine. Celovitost prenesenih datotek je treba preverjati z uporabo zgoščevalnih algoritmov (ISO, 2010, str. 7-8).

b) Uhajanje informacij

Informacije lahko iz organizacije uhajajo na različne načne, kot na primer preko aplikacij, ki omogočajo prenašanje datotek na spletne strežnike, preko nedovoljene prenosljive kode, ki se izvaja na informacijskih sistemih znotraj organizacije ali preko različne škodljive programske opreme opisane v prejšnjem odstavku. Varnostni mehanizmi, ki jih standard predlaga pri preprečevanju uhajanja informacij, so celovitost, kontrola dostopa in varnost komunikacije. Organizacija mora preprečiti neavtoriziran prenos prenosljive kode na varnih prehodih. Varni prehodi morajo dovoliti le prenos preverjene, digitalno podpisane prenosljive kode iz preverjenih, s strani organizacije dovoljenih spletnih strani. Koda mora biti podpisana z veljavnimi in s strani organizacije odobrenih digitalnih potrdil (ISO, 2010, str. 7-8).

c) Neavtorizirana uporaba in dostopi

Organizacija mora zagotoviti, da je vsaka uporaba in vsak dostop do aplikacij, sistemov in infrastrukture organizacije avtoriziran, saj lahko izguba kontrole nad temi elementi pripelje do goljufanja, zlorabe in izpada storitev ali dela informacijskega sistema. Varnostni mehanizmi, ki jih standard pri tem predlaga, so kontrola dostopa in preprečevanje zanikanja istovetnosti. Kontrola dostopa mora zagotoviti, da lahko uporabniki dostopajo zgolj do spletnih strani, aplikacij in storitev, ki so potrebne za izvajanje delovnih nalog uporabnika. Preprečiti mora dostop do neavtoriziranih storitev, uporabo nedovoljenih protokolov in dostop do storitev, ki omogočajo prenašanje velikih datotek. Preprečevanje zanikanja istovetnosti je treba zagotoviti z beleženjem in nadzorovanjem dostopov do vseh storitev, ki omogočajo prenašanje podatkov v smeri od uporabnika proti internetu. Organizacija mora v politiki dostopa do interneta natančno definirati pogoje uporabe dostopa do interneta in skrbeti za stalno ozaveščanje uporabnikov o varni rabi dostopov in informacijske infrastrukture organizacije (ISO, 2010, str. 7-8).

d) Odgovornost v primeru nespoštovanja regulatornih in zakonskih zahtev

Organizacija mora dobro poznati in v svojih politikah definirati vse regulatorne in zakonske zahteve ter s tem preprečiti nezavedno kršitev le-teh. Standard v tej točki zahteva vpeljavo beleženja in časovnega žigosanja za zagotavljanje preprečevanje zanikanja istovetnosti ter stalno ozaveščanje uporabnikov (ISO, 2010, str. 7-8).

e) Zmanjšanje razpoložljivosti omrežja

Organizacija mora preprečiti uporabo storitev in aplikacij, ki pri svojem delovanju uporabljajo veliko pasovne širine. Standard zahteva zagotavljanje celovitosti in razpoložljivosti omrežja z omejevanjem pasovne širine za pretočne vsebine, stalnim nadzorom omrežnih in sistemskih virov ter vzpostavitvijo sistema oziroma postopkov za upravljanje z ranljivostmi. Pri slednjem standard izpostavlja kritičnost nameščanja popravkov na vso omrežno infrastrukturo, preko katere organizacija dostopa do interneta ali je na drug način izpostavljena različnim javnim omrežjem (ISO, 2010, str. 7-8).

2.4.2.2 Medpodjetniško elektronsko poslovanje

Scenarij, ki ga standard predstavlja v tej točki, je namenjen organizacijam, ki preko interneta elektronsko poslujejo z drugimi organizacijami. Elektronsko poslovanje preko interneta prinaša vrsto novih tveganj, saj internet sam po sebi ne izpolnjuje visokih zahtev po razpoložljivosti, zanesljivosti in varnosti povezav med organizacijami. Organizacija mora zato na različne načine poskrbeti za ustrezno zmanjšanje tveganj, ki jih takšen način poslovanja prinaša, pri tem pa standard (ISO, 2010, str. 9-10) opisuje sledeče grožnje in priporočila za zmanjšanje z njimi povezanih tveganj.

a) Virusi in škodljiva programska koda

V primeru medpodjetniškega elektronskega poslovanja lahko vnos virusov in škodljive programske opreme vpliva na izpad sistemov in neavtoriziran dostop do občutljivih informacij. Varnostni mehanizmi in kontrole, ki jih standard pri tem predlaga, so enake kot v točki a poglavja 2.4.2.1.

b) Napad onemogočanja in porazdeljeni napad onemogočanja

Napad onemogočanja ali porazdeljeni napad onemogočanja storitev lahko pripelje do izpada omrežij ali portalov za izvajanje medpodjetniškega elektronskega poslovanja organizacije. Standard za zagotavljanje razpoložljivosti in zakrivanja predlaga izklop vseh neuporabljenih protokolov, komunikacijskih vrat in storitev na sistemih, ki so izpostavljeni drugim, predvsem javnim omrežjem, ter izločitev vseh informacij v pozdravnih in varnostnih sporočilih, ki bi lahko napadalcu dale informacije o sistemih organizacije (ISO, 2010, str. 9-10).

c) Notranji napad izveden s strani pooblaščenih poslovnih partnerjev

Pri uporabi medpodjetniškega elektronskega poslovanja je velika grožnja tudi zloraba dostopov s strani pooblaščenih uporabnikov. Varnostni mehanizmi in kontrole, ki jih standard pri tem predlaga, so kontrola dostopa in preprečevanje zanikanja istovetnosti. Organizacija mora pripraviti varnostno politiko upravljanja z dostopi, ki podrobno definira tudi dostope, vloge in odgovornosti poslovnih partnerjev. Na svoje sisteme mora namestiti prijavna opozorila, zagotoviti omejevanje pravic uporabnikom ter beleženje vseh transakcij, ki jih izvajajo uporabniki (ISO, 2010, str. 9-10).

d) Ponarejanje vsebine transakcij

Organizacija mora preprečiti ponarejanje vsebine transakcij in preprečevanje dostave sporočil s preprečevanjem zanikanja istovetnosti sporočila. Vzpostaviti mora sistem podrobnega beleženja vseh transakcij in uporabo digitalnih sporočil, s katerimi lahko dokazuje integriteto in istovetnost transakcije (ISO, 2010, str. 9-10).

2.4.2.3 Poslovanje s strankami

V tej točki je predstavljen scenarij elektronskega poslovanja organizacije s strankami. To vključuje elektronsko trgovanje, elektronsko bančništvo in elektronsko upravo. Organizacija mora poskrbeti za visoko stopnjo varnosti elektronskega poslovanja, torej za zaupnost, celovitost, učinkovit sistem overjanja uporabnikov, razpoložljivost in pa varnost komunikacije med strankinim sistemom in storitvijo organizacije. Pri tem mora upoštevati dejstvo, da je varnost sistemov na strani uporabnikov lahko slaba in vprašljiva, zaradi česar mora z izvedbo učinkovitih varnostnih kontrol in s pogoji poslovanja zagotovi varnost svojih storitev (ISO, 2010, str. 11). Standard (ISO, 2010, str. 11-12) v tem scenariju opisuje sledeče grožnje in priporočila za zmanjšanje le-teh.

a) Virusi in škodljiva programska koda

Organizacija mora v tem primeru še poskrbeti za učinkovito protivirusno zaščito in zaščito proti škodljivi programski kodi, saj je izpostavljena večjim tveganjem kot v prejšnjih primerih. Varnostni mehanizmi in kontrole, ki jih standard pri tem predlaga, so enake kot v točki a poglavja 2.4.2.1.

b) Neavtoriziran dostop

Organizacija mora uporabnikom preprečiti neavtoriziran dostop do zalednih podatkovnih strežnikov z izrabo različnih ranljivosti ter neavtoriziran dostop do sistemov in omrežja organizacije, preko katerih bi lahko uporabnik pridobil nepooblaščen dostop do internih podatkov organizacije. Za zagotovitev tega mora omejiti pravice pri dostopih čelnega dela

sistema do zalednih podatkovnih baz, čelni del sistema postaviti v demilitarizirano področje ter s pravili na požarnih pregradah omejiti dostop iz manj varnih omrežij v bolj varna omrežja. Dodatno varovanje čelnega dela sistema lahko organizacija izvaja tudi z vzpostavitvijo posredniških strežnikov med spletnimi strežniki in zunanjim omrežjem. Organizacija mora vpeljati varno registracijo uporabnikov, ki zagotavlja izdajo poverilnic za dostop do sistema le preverjenim uporabnikom. Preverjanje istovetnosti uporabnikov se mora izvajati z uporabo digitalnih potrdil, pametnih kartic, gesel ali biometričnih podatkov, sistem pa mora uporabnikom dodeljevati dostop glede na njihovo vlogo in s tem preprečiti neavtorizirano uporabo funkcij. Ker so uporabniški računi lahko tarča kraje identitet, mora organizacija preprečiti zajemanje uporabniških računov z uporabo različnih spletnih skript ter aplikacij in vzpostaviti sistem, ki preprečuje krajo internetne identitete z uporabo socialnega inženiringa. Vpeljati mora sistem šifriranja sporočil, informacij in podatkov, ki bo preprečil krajo informacij in morebitno kršitev avtorskih pravic. Vsi podatki in predvsem gesla morajo biti šifrirani, komunikacija med odjemalcem in strežnikom pa mora biti šifrirana z uporabo šifrirnega protokola SSLv3. Poleg šifriranja same komunikacije med odjemalcem in strežnikom pa standard zahteva zagotavljanje celovitost sejnih podatkov s šifriranjem piškotkov, uporabo časovnega žigosanja in digitalnim podpisovanjem občutljivih podatkov. Strežnike je treba zavarovati tudi s sistemom preverjanja celovitosti sistemskih datotek z uporabo kriptografskih metod. Vsi dostopi in poskusi dostopov morajo biti zabeleženi za namene odkrivanja in zajezitve napadov na sisteme organizacije (ISO, 2010, str. 11-12).

c) Napad onemogočanja in porazdeljeni napad onemogočanja

Grožnje, varnostni mehanizmi in kontrole so enake kot v točki b poglavja 2.4.2.2.

d) Ponarejanje vsebine transakcij

Grožnje, varnostni mehanizmi in kontrole so enake kot v točki d poglavja 2.4.2.2.

2.4.2.4 Storitve za napredno sodelovanje

Storitve za napredno sodelovaje omogočajo različne delovne skupine elektronskega sodelovanja med zaposlenimi s pomočjo glasovnega in video komuniciranja, komuniciranja preko klepetalnic in sistemov za izmenjavo elektronske pošte, skupno rabo dokumentov ter uporabo različnih okolij in storitev za spletno sodelovanje. Standard deli uporabo takšnih storitev na notranjo uporabo, kjer so storitve omejene le na uporabnike znotraj organizacije in zunanjo uporabo, kjer so storitve omogočene tudi drugim uporabnikom. Slednje je z vidika varnostni veliko bolj kritično, saj je storitev za napredno sodelovanje izpostavljena zunanjim omrežjem. Druga delitev teh storitev je glede na tip izvedbe storitve, ki je lahko narejena in nameščena v informacijskem sistemu organizacije ali najeta pri ponudniku (ISO, 2010, str. 13). Standard (ISO, 2010, str. 14) v tem scenariju opisuje sledeče grožnje in priporočila za zmanjšanje z njimi povezanih tveganj.

a) Neavtoriziran dostop

Neavtoriziran dostop lahko vodi do razkritja zaupnih podatkov, kršenja avtorskih pravic, izpostavitve uporabnikov neželeni vsebini, kraje identitet ali odkritja sledenja uporabnikov s pregledovanjem vzorcev uporabe. Standard za zmanjšanje tveganj, povezanih z zapisanimi grožnjami, predlaga vzpostavitev kontrole dostopa do aplikacij, omrežij in sistemov za shranjevanje podatkov glede na vlogo uporabnika. Uporabnike z različnimi vlogami je treba glede na vlogo razporediti v ločena navidezna lokalna omrežja, ki jim omejujejo dostope na podlagi dodeljenih vlog. Identifikacijo uporabnikov je treba izvajati z uporabo naprednih sistemov overjanja, prav tako pa je treba zagotoviti zaupnosti na nivoju podatkov in komunikacije z uporabo šifriranja. Storitveni strežniki morajo biti zaščiteni z uporabo gostiteljskih sistemov za zaznavanje in preprečevanje vdorov ter sistemi za preprečevanje zanikanja istovetnosti (ISO, 2010, str. 14).

b) Virusi in škodljiva programska koda

Pri deljenju datotek in skupnem dostopu do podatkov se pojavi tudi tveganje za širitev virusov in škodljive programske kode, kar vpliva na celovitost podatkov in informacijskega sistema organizacije. Za zmanjšanje tveganja standard predlaga uporabo programske opreme za prenos zaslonske slike, kar prepreči, da bi uporabnik lastni sistem izpostavil tveganju prenosa virusa ali škodljive programske kode (ISO, 2010, str. 14).

c) Zmanjšanje razpoložljivosti omrežja

Vpliv na razpoložljivost omrežja je lahko nameren ali nenameren. Namerno jo lahko zmanjšajo različni tipi napadov na ranljivosti v protokolih, ki zagotavljajo uporabo storitev naprednega sodelovanja, nenamerno pa množična uporaba storitve. Standard v tej točki predlaga uporabo navideznega omrežja za shranjevanje podatkov, s čimer zagotovimo boljšo razpoložljivost in varnost podatkov v mirovanju. Poleg tega standard zahteva tudi vzpostavitev sistema za nadzor kršenja pravic dostopa do aplikacij in omrežne opreme ter vpeljavo programske opreme in orodij, ki preprečujejo kopiranje, brisanje, tiskanje ter zapisovanje informacij na prenosne medije (ISO, 2010, str. 14).

2.4.2.5 Segmentacija omrežij

Segmentacija omrežij je ločevanje enega omrežja na več omrežij, kar organizaciji omogoči vzpostavitev različnih varnostnih področij. Standard predlaga ločevanje omrežij na omrežja za administracijo in vzdrževanje informacijskih sistemov, omrežja podatkovnih strežnikov in omrežja za uporabnike. Ločevanje omrežij priporoča tudi v multinacionalnih organizacijah, kjer z ločevanjem po državah lažje zagotovimo skladnost z lokalnimi zakonskimi in regulatornimi zahtevami. Neskladnost je v tej točki identificirana kot tveganje, ki ga mora organizacija zmanjšati z zagotavljanjem zaupnosti in zakrivanjem. Organizacija mora zato vzpostaviti

primerne varnostne politike ter uporabnike stalno ozaveščati o zakonskih zahtevah, dovoljeni in zahtevani uporabi kriptografskih metod, načinih hrambe podatkov in izvajanju zakonitega prestrezanja. Drugo tveganje je uhajanje oziroma izguba podatkov. To mora organizacija preprečiti z uporabo varnih prehodov, posredniških strežnikov in šifriranjem podatkov ter na ta način zagotoviti celovitost in kontrolo dostopa do podatkov (ISO, 2010, str. 14-15).

2.4.2.6 Omrežna podpora domače in male poslovalnice

Veliko domačih in malih poslovalnic (v nadaljevanju poslovalnic) potrebuje dostop do različnih informacijskih virov znotraj omrežja organizacije. Te povezave organizacije navadno vzpostavijo z namenom znižanja stroškov, kar po drugi strani negativno vpliva na zagotavljanje varnosti. Varovanje povezav s poslovalnicami je še posebej kritično, ker navadno poslovalnice uporabljajo isto omrežje za poslovne in zasebne namene (ISO, 2010, str. 16). Standard (ISO, 2010, str. 16-17) v tem scenariju opisuje sledeče grožnje in priporočila za zmanjšanje z njimi povezanih tveganj na sistemih znotraj organizacije in sistemih v poslovalnicah.

a) Neavtoriziran dostop

V primerih povezovanja zunanjih omrežij z notranjim omrežjem organizacije je treba poskrbeti za dobro kontrolo dostopa, overjanje uporabnikov in varovanje komunikacij. Omrežje organizacije je lahko izpostavljeno tveganjem neavtoriziranega dostopa zaradi pomanjkljivih nastavitev na omrežnih napravah v poslovalnici, uporabe razcepljenih tunelov, uporabe uporabniških računov za goste ter privzetih nastavitev. Varnostni mehanizmi in kontrole, ki jih standard predlaga v tem scenariju, so vezane predvsem na zagotavljanje višje stopnje varnosti v poslovalnicah. S preprečitvijo uporabe praznih gesel, anonimne prijave ali prijave z računom za goste je treba zagotoviti varno overjanje uporabnikov na delovnih postajah. Na delovne postaje je treba namestiti programsko požarno pregrado, ki dovoljuje le vzpostavljanje povezav iz delovne postaje proti omrežju, ter onemogočiti vse omrežne vmesnike in storitve, ki niso potrebni za delovanje sistema. Na omrežnih prehodih je treba vzpostaviti varno navidezno zasebno omrežno povezavo z organizacijo in s primerno tehnologijo ter zasnovo poskrbeti za zagotavljanje varnosti pri morebitni uporabi razcepljenih tunelov. Organizacija mora periodično preverjati nastavitve opreme v poslovalnicah in s tem zagotoviti skladnost z zahtevami organizacije (ISO, 2010, str. 16-17).

b) Virusi in škodljiva programska koda

Podobno kot v prejšnji točki je notranje omrežje organizacije lahko, zaradi slabih varnostnih kontrol na opremi in delovnih postajah poslovalnice, izpostavljeno tveganju vnosa virusov in škodljive programske kode. Organizacija mora za zagotavljanje celovitosti in razpoložljivosti zagotoviti redno nameščanje varnostnih popravkov, redno nadgrajevanje programske opreme, namestitev in redno nadgrajevanje protivirusne programske opreme na delovnih postajah uporabnikov, uporabo gostiteljskih sistemov za zaznavanje in preprečevanje vdorov ter stalno preverjanje vseh shranjenih datotek in podatkov proti virusom, škodljivi programski kodi in

trojanskim konjem. Vse nastavitve in datoteke mora organizacija varno hraniti za primere incidentov in morebitne potrebe po obnovi varnostnih kopij (ISO, 2010, str. 16-17).

c) Nepooblaščeno razkritje občutljivih informacij

Najbolj pogost razlog za nepooblaščeno razkritje občutljivih informacij je pomanjkanje ozaveščenosti uporabnikov, saj uporabniki napačno ocenjujejo varnost omrežij poslovalnice in organizacije ter povezave med omrežjema. Podatki se zaradi tega največkrat hranijo in prenašajo v nešifrirani obliki, zato mora organizacija zagotoviti šifriranje podatkov v mirovanju in gibanju, uporabnike pa redno ozaveščati o najboljših praksah varovanja podatkov in informacij (ISO, 2010, str. 17).

2.4.2.7 Mobilne komunikacije

Scenarij predvideva uporabo mobilnih naprav za dostopanje do informacijske infrastrukture organizacije. Ker uporabniki mobilne naprave največkrat uporabljajo tako za poslovno kot zasebno rabo, so informacijski in omrežni sistemi organizacije izpostavljeni različnim notranjim in zunanjim tveganjem. Standard (ISO, 2010, str. 18-19) opisuje sledeče grožnje ter kontrole in tehnike snovanja, ki tveganja, povezana s temi grožnjami, zmanjšujejo.

a) Neavtoriziran dostop do informacij shranjenih na mobilni napravi

Organizacija mora vzpostaviti zadovoljivo raven kontrole dostopa in sistema overjanja ter preprečiti možnost zanikanja istovetnosti. Preko programov ozaveščanja mora uporabnikom predstaviti zahteve za zaščito občutljivih informacij na mobilnih napravah, pod katere spadajo fizični nadzor nad napravo, uporaba močnih gesel in pazljivost pri dostopu do neznanih brezžičnih omrežij, preko katerih bi lahko napadalci s prestrezanjem prišli do podatkov med prenosom. Organizacija mora s tehničnimi kontrolami preprečiti uporabo privzetih nastavitev na mobilnih napravah, uporabo šibkih gesel, omogočiti beleženje dostopov, samodejno zaklepanje mobilne naprave v času mirovanja ter namestitev požarnega zidu. Če je potrebno, lahko organizacija zahteva tudi uporabo mobilnih naprav izključno v poslovne namene (ISO, 2010, str. 18-19).

b) Neavtorizirano razkritje občutljivih podatkov in informacij o lokaciji

Pomanjkljive nastavitve mobilnih naprav in napačna uporaba lahko pripeljeta do razkritja občutljivih podatkov ali informacij o lokaciji naprave in uporabnika. To je izvedljivo s prisluškovanjem nešifriranemu podatkovnemu toku, uporabi storitev, ki ne zagotavljajo ustrezne zaščite podatkov ali z zavrženjem naprave brez ustreznega predhodnega brisanja podatkov. Organizacija mora za zmanjšanje tveganj, povezanih z naštetimi grožnjami, zagotoviti zaupnost, ustrezne mehanizme overjanja, varno komuniciranje in zakrivanje. Na mobilnih napravah mora vzpostaviti uporabo varnih gesel ter šifriranje shranjenih podatkov,

šifriranje podatkov med prenosom z uporabo varnih navideznih zasebnih omrežij ter varne sinhronizacije podatkov. Tako uporabniki kot organizacija se morajo izogibati uporabi storitev, ki ne zagotavljajo šifriranja podatkov med prenosom. Če tega ni mogoče zagotoviti, mora organizacija od ponudnika storitve zahtevati zagotavljanje zaupnosti na drugih nivojih. Če organizacija zahteva uporabo lokacijskih storitev, mora pred tem pridobiti soglasje uporabnikov. Pred prenehanjem uporabe oziroma zavrženjem mobilne naprave je treba zagotoviti varno brisanje vseh občutljivih podatkov na mobilni napravi (ISO, 2010, str. 18-19).

c) Neavtorizirano spreminjanje in brisanje informacij ter programske opreme

Grožnji, povezani z neavtoriziranim spreminjanjem in brisanjem informacij ter programske opreme, sta vnos zlonamerne programske opreme in izraba ranljivosti v operacijskem sistemu mobilne naprave. Namestitev zlonamerne programske opreme na mobilno napravo se navadno izvede ob namestitvi različne programske opreme iz neavtoriziranih virov. Organizacija mora zato vzpostaviti sistem, ki uporabnikom omogoča zgolj nameščanje programske opreme dosegljive preko distribucijskega sistema organizacije. Namestitveni paketi programske opreme morajo biti digitalno podpisani. Drugo tveganje je treba zmanjšati z izklopom neuporabljenih brezžičnih vmesnikov, storitev in aplikacij, stalnim nadgrajevanjem in nameščanjem popravkov operacijskega sistema na mobilnih napravah, namestitvijo protivirusne zaščite na mobilne naprave in zagotavljanjem varnega brisanja vseh občutljivih podatkov na mobilnih napravah pred prenehanjem uporabe ali zavrženjem (ISO, 2010, str. 18-19).

d) Neželena elektronska sporočila

Varnostne grožnje, ki jih standard opisuje v tej točki, so visoki stroški uporabe mobilnega omrežja, napadi z ribarjenjem in napadi onemogočanja. Vse tri grožnje so posledica prejema neželenih elektronskih sporočil. Standard pri tem predlaga učinkovito kontrolo dostopa. Organizacija mora zagotoviti filtriranje vsebine elektronskih sporočil ter preko programa ozaveščanja uporabnikov uporabnike naučiti, kako se odzvati pri prejemu neželenih elektronskih sporočil (ISO, 2010, str. 18-19).

e) Kraja ali izguba mobilne naprave

V primeru kraje ali izgube mobilne naprave je organizacija izpostavljena tveganjem izgube in razkritja podatkov na mobilni napravi. Za zmanjšanje verjetnosti uresničitve teh groženj mora organizacija vzpostaviti centralni nadzorni sistem za nadzor sredstev in skladnosti z varnostno politiko organizacije. Zagotoviti mora varno periodično varnostno kopiranje vseh pomembnih podatkov ter ustrezno zaščito vseh podatkov na mobilnih napravah. Standard pri zaščiti zaupnosti podatkov predvideva tudi vzpostavitev sistema za oddaljeno upravljanje sredstev, ki mora omogočati oddaljeno zaklepanje mobilnih naprav ali oddaljeno uničenje podatkov na mobilni napravi (ISO, 2010, str. 18-19).

2.4.2.8 Omrežna podpora za potujoče uporabnike

Organizacije, ki morajo poslovnim potnikom omogočiti dostop do notranjih virov, se morajo zavedati tveganj, ki nastajajo pri uporabi oddaljenih dostopov. Standard pri tem opozarja na pomanjkljivo zagotavljanje varnosti pri uporabi storitev za oddaljeni dostop, ki jih ponujajo različni ponudniki na trgu. Tveganji, identificirani v tem scenariju, sta neavtoriziran dostop in zmanjšanje razpoložljivosti omrežja (ISO, 2010, str. 20).

S kontrolo dostopov, overjanjem in zagotavljanjem varne komunikacije ter zaupnosti mora organizacija preprečiti neavtoriziran dostop do notranjih virov in podatkov organizacije. Tveganje neavtoriziranega dostopa do podatkov se lahko uresniči z neavtoriziranim dostopom do podatkov, shranjenih na napravi uporabnika, z zlorabo storitev oddaljenega dostopa ali ogrožanjem varnih prehodov, ki ščitijo interno omrežje organizacije. Varnostne kontrole je treba vzpostaviti tako na omrežju organizacije kot na končni napravi, ki omogoča uporabnikom dostop do organizacije. Standard zahteva uporabo šifriranja podatkov, shranjenih na napravah uporabnikov, naprednih tehnik overjanja uporabnikov, vzpostavitvijo namenskih varnih strežnikov za oddaljen dostop, ki zagotavljajo zaščito dostopov in transporta podatkov z uporabo TLS/SSLv3 protokola ter uporabo varnih navideznih zasebnih omrežij, vzpostavljenih med napravo uporabnika in varnim prehodom organizacije. Slednje lahko organizacija zagotovi z izvedbo navideznih zasebnih omrežij na drugem ali tretjem OSI nivoju ali z izvedbo aplikacijskih navideznih zasebnih omrežij na sedmem OSI nivoju (ISO, 2010, str. 20).

Pri zmanjšanju razpoložljivosti omrežja se standard navezuje na pričakovanja uporabnikov po hitrosti delovanja oddaljenega dostopa. Ta je odvisna od hitrosti povezave, ki jo v tistem trenutku uporablja uporabnik, zato standard predlaga spodbujanje ponudnikov dostopov k zagotavljanju zadostne razpoložljivosti in zmogljivosti omrežij ali k podpisu sporazuma o nivoju storitve med ponudniki dostopov in organizacijo (ISO, 2010, str. 20).

2.4.2.9 Zunanje izvajanje storitev

Pri uporabi zunanjega izvajanja storitev je organizacija izpostavljena različnim tveganjem. Standard v tej točki izpostavlja predvsem grožnje iz naslova dostopa zunanje organizacije do notranjih virov organizacije ob zagotavljanju izvajanja storitve in podpori. Največkrat se pri teh dostopih uporabljajo privilegirani računi, ki omogočajo popolni nadzor nad izpostavljenimi sistemi organizacije (ISO, 2010, str. 21). Standard (ISO, 2010, str. 21-22) pri zunanjem izvajanju storitev izpostavlja naslednje grožnje in z njimi povezana tveganja.

a) Posredni neavtoriziran dostop do internih sistemov

Izvajalci zunanjega izvajanja, ki morajo imeti za zagotavljanje delovanje storitev in podpore tudi dostop do določenih notranjih sistemov organizacije, lahko z zlorabo svojega dostopa posredno preko teh sistemov dostopajo do drugih sistemov znotraj omrežja organizacije.

Organizacija mora zato zagotoviti primerno kontrolo dostopa, overjanje uporabnikov in preprečevanje zanikanja istovetnosti. Vzpostaviti mora sistem dodeljevanja poimenskih uporabniških imen in se izogibati dodelitvi enotnega uporabniškega imena za skupino zunanjih izvajalcev. Dostop do sistemov mora omogočati napredne metode overjanja za vse oddaljene dostope s privilegiranimi računi. Overjanje uporabnikov je treba zagotoviti pri uporabi konzolnih dostopov na komunikacijsko in informacijo opremo. Za preprečevanje zanikanja istovetnosti mora organizacija zagotoviti beleženje vseh dostopov in aktivnosti izvajalcev ter periodično pregledovanje vseh zapisov (ISO, 2010, str. 21-22).

b) Neavtorizirano razkritje občutljivih podatkov s strani ponudnika zunanjega izvajanja

Organizacija je odgovorna za zagotavljanje zaupnosti podatkov, do katerih dostopajo zunanji izvajalci, zato mora z uporabo šifriranja podatkov, nadzorovanjem in revidiranjem revizijskih sledi, izvajanjem varnostnega ozaveščanja in pogodbenimi obveznostmi preprečiti neavtorizirano razkritje občutljivih podatkov s strani ponudnika zunanjega izvajanja. To se največkrat zgodi ravno zaradi pomanjkanja ozaveščenosti zunanjih izvajalcev ter uporabe nešifrirane komunikacije med organizacijo in zunanjimi izvajalci (ISO, 2010, str. 21-22).

c) Vnos zlonamerne programske opreme v razvojno okolje

Standard v tej točki ugotavlja, da lahko zaradi neustrezne varnosti pri razvoju in nadgrajevanju programske opreme, nešifrirani komunikaciji pri prenosu datotek in podatkov ter uporabi spletnih orodij za sodelovanje, ki ne zagotavljajo dovolj visokega nivoja varnosti, v okolje organizacije zunanji izvajalci namerno ali nenamerno vnesejo zlonamerno programsko opremo. Za preprečevanje le-tega, mora organizacija slediti praksam varnega programiranja, vzpostaviti sistem upravljanja s spremembami ter zagotoviti stalno nadgrajevanje protivirusne zaščite na vseh izpostavljenih sistemih (ISO, 2010, str. 21-22).

d) Odgovornost v primeru neupoštevanja regulatornih zahtev

Organizacija lahko zunanje izvajanje storitev najema tudi pri izvajalcih v drugih državah. Tveganji, ki jih standard v tem primeru izpostavlja, sta slabo poznavanje zakonskih in regulatornih zahtev s strani izvajalcev ter morebitne ohlapne zakonske in regulatorne zahteve v državi zunanjih izvajalcev in posledično neskladje obdelave podatkov z zahtevami. Organizacija mora tveganja zmanjšati z ozaveščanjem zunanjih izvajalcev, uporabo dovoljenih kriptografskih metod ter mehanizmov za zagotavljanje zakrivanja podatkov med prenosom (ISO, 2010, str. 21-22).

2.5 ISO/IEC 27033-4:2014

ISO/IEC 27033-4:2014 je časovno gledano zadnji izdani del standarda ISO/IEC 27033. Izdan je bil začetek leta 2014 in v celoti zamenjuje ISO/IEC 18028-3, ki je bil izdan leta 2005. Naziv

četrtega dela standarda je Varovanje komunikacije med omrežji z uporabo varnostnih prehodov (ISO, 2014, str. IV).

2.5.1 Obseg in struktura

Standard v četrtem delu podaja smernice in zahteve za vzpostavitev varovanja komunikacij med različnimi omrežji z uporabo varnostnih prehodov. V prvih dveh poglavjih predstavlja načine identifikacije in analize tveganj, povezanih z varnimi prehodi ter varnostne zahteve, ki jih potrebujemo za vzpostavitev varnih prehodov med različnimi omrežji organizacije. V nadaljevanju so predstavljene varnostne kontrole in omrežni scenariji, s katerimi se navadno srečujemo pri vzpostavitvi varnostnih prehodov ter tehnike snovanja varnega komunikacijskega omrežja z uporabo varnih prehodov. V zadnjem poglavju standard podaja smernice za izbor primerne opreme glede na grožnje in zahteve identificiranje v predhodnih poglavjih (ISO, 2014, str. III-V).

2.5.2 Priporočila in zahteve

Organizacije, poleg segmentacije notranjega omrežja, svoje omrežje povezujejo tudi z različnimi tipi javnih omrežij in z omrežji drugih organizacij. Vsako tako omrežje spada v svoje varnostno območje, ki narekuje zahteve po varovanju omrežja oziroma sistemov znotraj omrežja. Varnostno območje vzpostavimo s filtriranjem in nadzorovanjem komunikacijskega prometa med dvema ali več omrežji z uporabo varnostnih prehodov. Poznamo več različnih tipov varnostnih prehodov, kot na primer aplikacijske in klasične požarne pregrade, sistemi za zaznavanje in preprečevanje vdorov, posredniški strežniki itd. Te naprave delujejo na različnih nivojih komunikacijskega protokola ter posledično omogočajo različne pristope k filtriranju in nadzorovanju prometa (ISO, 2014, str. 4-5). V nadaljevanju bom predstavil priporočila in zahteve standarda za izbiro in namestitev varnostnih prehodov.

2.5.2.1 Varnostne grožnje

Podobno kot v prejšnjih delih standarda, je v prvem koraku treba identificirati in analizirati varnostne grožnje. Namen varnostnega prehoda je, da omrežje, ki ga varuje, ščiti pred vdori oziroma neavtoriziranim dostopom iz notranjih in zunanjih omrežij. Ključne varnostne grožnje, ki jih standard izpostavlja, so neavtorizirano spreminjanje ali razkritje podatkov, neavtorizirane spremembe nastavitev različnih sistemov, neavtorizirana uporaba virov ali sredstev organizacije, neavtoriziran prenos vsebine, kot na primer prenos virusov in zlonamerne programske opreme, zloraba virtualizacije ter onemogočanje ali porazdeljeno onemogočanje storitev (ISO, 2014, str. 6).

2.5.2.2 Varnostne zahteve

Z varnostnimi prehodi lahko organizacija zagotavlja različne varnostne mehanizme za

varovanje omrežja. Relacije med varnostnimi grožnjami in različnimi varnostnimi zahtevami oziroma mehanizmi, ki jih zagotavljamo z uporabno varnostnih prehodov, so predstavljene v tabeli 1.

Tabela 1: Relacije med tveganji in varnostnimi zahtevami

Grožnje	**Varnostne zahteve, ki jih omogočajo varnosti prehodi**						
	Logična segmentacija omrežja	Omejevanje in analiza prometa, ki se prenaša med logičnimi omrežji	Kontrola dostopa v in iz omrežja organizacije z nadzorovanjem povezav ali uporabo posredovanja operacij na izbranih aplikacijah	Uveljavljanje omrežne varnostne politike organizacije	Beleženje prometa za namene revizije	Zakrivanje notranjega omrežja, naprav in aplikacijske arhitekture	Omogoča upravljanje omrežja
Zavračanje storitve avtoriziranim uporabnikom		X		X	X		X
Neavtorizirana sprememba podatkov	X	X	X	X	X		X
Neavtorizirano razkritje podatkov	X	X	X	X	X		X
Neavtorizirano spreminjanje nastavitev sistemov			X	X	X	X	X
Neavtorizirana uporaba virov in sredstev organizacije	X	X	X	X	X	X	X
Neavtoriziran prenos vsebine	X	X	X	X	X	X	X
Zloraba virtualizacije	X	X	X	X	X		X
Ohromitev ali porazdeljena ohromitev storitev		X		X	X		X

Vir: ISO, ISO/IEC 27033-4:2014, 2014, str.7.

2.5.2.3 Varnostne kontrole

V tej točki standard predstavlja različne varnostne kontrole ter priporočila in zahteve za njihovo uporabo. Organizacija mora za vsak posamezni varnostni prehod vzpostaviti dokumentacijo, ki mora vsebovati natančna pravila upravljanja z varnostnim prehodom ter omejitve in pravila, pod katerimi je dovoljen prenos podatkov preko varnostnega prehoda. Ta pravila morajo odražati zahteve varnostne politike organizacije, varnostni prehodi pa morajo z identifikacijo in overjanjem uporabnikov dovoljevati le dostope do sistemov, kot to določa politika. Poleg tega morajo varnostni prehodi omogočati tudi beleženje vseh dostopov uporabnikov do sistemov in storitev. Ker so varnostni prehodi izpostavljeni različnim tveganjem vnosa zlonamerne

programske opreme in virusov, je treba zagotoviti redno preverjanje varnostnih prehodov s protivirusno programsko opremo ter opremo za zaznavanje zlonamerne programske opreme in skrbno nameščanje varnostnih popravkov in novih različic operacijskega sistema (ISO, 2014, str. 8). Varnostne kontrole, ki jih omogočajo varnosti prehodi, so filtriranje paketov brez upoštevanja stanja povezave, nadzor paketov z upoštevanjem vseh stanj, aplikacijske požarne pregrade, filtriranje vsebine, sistemi za zaznavanje in preprečevanje vdorov in upravljanje varnosti preko vmesnika za aplikacijsko programiranje. Posamezne kontrole so splošno znane, zato jih v magistrskem delu ne bom posebej predstavljal.

2.5.2.4 Tehnike snovanja

V tej točki standard opisuje komponente varnostnih prehodov ter podaja primere uvajanja kontrol z varnostnimi prehodi.

Komponente varnostnih prehodov standard deli na omrežna stikala, usmerjevalnike, prehode, ki analizirajo promet na aplikacijskem nivoju, varnostne naprave in funkcije nadzorovanja. Standard jih v tem delu opisuje na straneh 11 in 12. Ker je delovanje naštetih komponent splošno znano, jih v magistrskem delu ne bom posebej predstavljal in bom predstavljal le uvajanje kontrol varnostnih prehodov.

Standard uvajanje kontrol varnostnih prehodov opisuje preko primerov, kjer opredeli predvsem uporabo posameznega varnostnega prehoda. Najprej je predstavljena arhitektura z uporabo požarnih pregrad, ki omogočajo filtriranje paketov brez upoštevanja stanja povezave in nadzor paketov z upoštevanjem vseh stanj. Ker požarne pregrade analizirajo zgolj tretji in četrti OSI nivo paketov, so zelo hitre in prilagodljive, uporabne pa so predvsem kot varnostni prehodi med zunanjimi omrežji organizacije in javnimi omrežji, kjer je hitrost pomembnejša od zagotavljanja varnosti na aplikacijskem nivoju. Naslednja stopnja zagotavljanja varnosti je arhitektura z uporabo t. i. dvo ali več domskega prehoda. Te naprave se imenujejo aplikacijski posredniki oziroma prehodi, ki povezujejo dve ali več omrežij. Posebnost teh naprav je, da se paketi med omrežji ne posredujejo neposredno, kot v primeru požarnih pregrad. Naprava v posameznem omrežju mora komunicirati neposredno s prehodom oziroma posredniškim strežnikom, ki proti ciljni napravi vzpostavi novo sejo, preko katere posreduje podatke. To omogoča višjo stopnjo varnosti, saj naprave v posameznem omrežju niso neposredno dosegljive napravam v drugih omrežjih. Tak način delovanja omogoča tudi zakrivanje arhitekture notranjega omrežja, slaba stran tovrstnih naprav pa je, da omogočajo samo posredovanje storitev oziroma protokolov, ki jih programsko podpirajo. Podoben tip varovanja nam omogočata tudi arhitekturi zaslonjenega gostitelja in zaslonjenega omrežja. V obeh primerih z usmerjevalnikom in požarno pregrado ščitimo enega ali več gostiteljev. Promet, ki je posredovan bodisi s strani zunanjega bodisi s strani notranjega omrežja proti zaščitenim gostiteljem, je preko usmerjevalnika posredovan požarni pregradi ali aplikacijskemu posredniku, ta pa s kombinacijo filtriranja paketov in pregledovanja vsebine ščiti gostiteljski strežnik oziroma aplikacijo. Arhitektura omrežja mora zagotavljati, da je iz zunanjih omrežij

nemogoče neposredno posredovati promet do gostiteljskega strežnika. Tako zaščitena omrežja običajno imenujemo demilitarizirano področje (ISO, 2014, str. 12-16).

2.5.2.5 Smernice za izbor opreme

V tej točki standard podaja smernice za izbor opreme, ki organizaciji zagotavlja varovanje omrežij. V prvi vrsti poudarja pomembnost ločevanja javnih omrežij od internega omrežja organizacije ter segmentacijo internega omrežja z varnostnimi prehodi. Izbrani varnostni prehodi morajo izpolnjevati vse zahteve identificirane v točki 2.5.2.2. Standard pri tem opozarja, da mora biti organizacija pozorna na notranje in zunanje grožnje in pri tem upoštevati tudi človeški dejavnik. Pri načrtovanju in izbiri naprav je treba slediti enostavnim zasnovam ter uporabi komponent ali naprav v skladu z njihovimi funkcionalnostmi (ISO, 2014, str. 16-17).

Pri izbiri opreme standard (ISO, 2014, str. 16) predpisuje naslednje smernice: varnostni prehod mora omogočati izvajanje in varovanje oddaljenih dostopov, protivirusno pregledovanje, filtriranje prenosa potencialno nevarnih izvršljivih datotek v različnih protokolih, vzpostavitev varnih navideznih zasebnih omrežij, integracijo s sistemi za pregledovanje vsebine ter sistemi za zaznavanje in preprečevanje vdorov. Te dopolnjuje še z naslednjimi smernicami in priporočili, ki se nanašajo na različne komponente in lastnosti prehodov:

a) Izbira arhitekture varnostnega prehoda in ustreznih komponent

Izbira varnostnega prehoda mora odražati poslovne zahteve in zahteve po varnosti. Pri definiranju arhitekture je treba upoštevati tehnike snovanja, zapisane v prejšnjem poglavju (ISO, 2014, str. 17).

b) Izbira strojne in programske platforme

Pri izbiri strojne in programske opreme je treba upoštevati zahteve po zmogljivosti, zanesljivosti, učinkovitosti in seveda uporabnosti v predvideni varnostni arhitekturi. Standard priporoča tudi pregled znanih ranljivosti programske opreme (ISO, 2014, str. 17).

c) Nastavitve naprav

Standard (ISO, 2014, str. 17-18) v tej točki za zagotavljanje varnosti omrežja in samega varnostnega prehoda predlaga uporabo komutiranega omrežja pri vzpostavljanju arhitekture zaslonjenega omrežja ali demilitarizirane cone, statičnega usmerjanja med usmerjevalniki in varnostnimi prehodi, onemogočenje izvornega usmerjanja, namestitev izključno programske opreme in storitev, ki so nujno potrebne za izvajanje želenih funkcij, zaprtje ali filtriranje protokolnih vrat, ki niso v uporabi, izklop vmesnikov za analizo prometa, če niso v uporabi, uporabo gesel na vseh vmesnikih, zavračanje vseh paketov, ki vsebujejo podatke o ohlapnem izvornem usmerjanju usmerjevalnega protokola RIP, zagotovitev ustrezne zmogljivosti

prevajanja omrežnih naslovov, transparentnega obratovanja varnostnega prehoda, kontrolo dostopa z uporabo identifikacije in overjanja, zagotavljanje beleženja vseh skrbniški dogodkov in prometa, utrjevanje operacijskega sistema platforme ter zagotavljanje izvajanja skrbniških opravil v primeru izpada varnostnega prehoda.

d) Varnostne lastnosti in nastavitve

Standard (ISO, 2014, str. 18-19) v tej točki opisuje naslednje minimalne zahteve, ki jih mora omogočati varnostni prehod:

- Aplikacijska požarna pregrada mora omogočati:

- podporo za najbolj uporabljanje internetne protokole, kot so HTTP, FTP, Telnet, SMTP in NNTP,
- podporo za nadaljnje storitve,
- odporo za posredovanje generičnih protokolov in storitev,
- HTTP posredovanje mora omogočati tudi posredovanje HTTPS prometa,
- zavračanje paketov BGP protokola,
- podpora protokolom za dinamično usmerjanje,
- podpora za spletne storitve, kot na primer SOAP/XML,
- podpora za posredovanje poslovnih aplikacij,
- zaznavanje in identifikacijo aplikacij znotraj paketnega toka, kot na primer ugnezdeni prenos videa, neposredno sporočanje itd.,
- pregledovanje dohodnega prometa preko navideznih zasebnih omrežij proti zlonamerni programski opremi,
- zmožnost posredovanja, blokiranja in izpuščanjem povezav ali paketov.

- Naprave za filtriranje paketov morajo omogočati najmanj:
- filtriranje paketov glede na podatke v paketu,
- filtriranje paketov glede na izvorne in ponorne IP naslove,
- filtriranje paketov glede na izvorna in ponorna protokolna vrata za protokola TCP in UDP,
- filtriranje paketov glede na smer povezave, navznoter ali navzven.

- Naprave za filtriranje paketov in nadzor paketov z upoštevanjem vseh stanj morajo omogočati najmanj:

- filtriranje storitev in protokolov NFS, NIS, RPC, RIP, OSPF, DNS in WAIS,
- zaznavanje določenih napadov na storitve, kot na primer napad s poplavljanjem s SYN paketi,
- preprečevanje ugibanja sekvenčne številke TCP paketa,
- onemogočiti t.i. napad s smrtnim ping-om,
- vezanje uporabe FTP ukazov na pravice uporabnika,
- shranjevanje informacij o kontekstu, kot na primer preverjanje dinamično dodeljenih

protokolnih vrat,
- Filtriranje objektov, kot so domene, skupine, objekti navideznih zasebnih omrežij itd.,
- preprečevanje nekaterih napadov s prestrezanjem seje.

- Ostale nastavitve in lastnosti:

- alarmiranje v primerih zaznave napadov s sledenjem zapisov ali integracijo s sistemov za zaznavanje vdorov,
- zaradi narave SOAP komunikacijskih mehanizmov, ki lahko prehajajo različne požarne pregrade in aplikacijske posrednike brez pregleda komunikacije, je treba zagotoviti varnost te komunikacije z uporabo navideznih zasebnih omrežij ali podobnih rešitev.

e) Administracija

Varnostni prehod mora zagotavljati varno identifikacijo in overjanje skrbnikov z deljenjem vlog, šifriranjem komunikacije med delovno postajo skrbnika in varnostnim prehodom, možnostjo upravljanja varnostnih prehodov preko centralnega sistema, testiranja integritete sistema varnostnega prehoda ter alarmiranja skrbnikov preko različnih poti, kot so na primer elektronska in SMS sporočila, pošiljanje alarmov na centralni alarmni sistem itd. Poleg teh zahtev mora sistem omogočati tudi enostavno in prilagodljivo upravljanje (ISO, 2014, str. 19).

f) Beleženje

Beleženje dogodkov in dostopov je zelo pomembno za zagotavljanje komunikacijske sledi. Varnostni prehod mora omogočati čim bolj natančno beleženje paketov, ki so bili posredovani ali zavrženi. Zapisi morajo biti zaščiteni pred nepooblaščenim dostopom, brisanjem in spreminjanjem, vsak zapis pa mora vsebovati tudi natančen datum in uro, ki morata biti na varnostnem prehodu stalno sinhronizirana z uporabo protokola za omrežno sinhronizacijo časa (ISO, 2014, str. 19).

g) Revizijska sled

Poleg beleženja mora varnostni prehod omogočati tudi revizijsko sled, ki zagotavlja minimalne varnostne zahteve glede zaupnosti, celovitosti, dostopnosti, overjanja, odgovornosti in preprečevanja zanikanja istovetnosti (ISO, 2014, str. 20).

h) Urjenje in izobraževanje

Pri izbiri varnostnega prehoda je treba zagotoviti periodično izobraževanje in urjenje skrbnikov. Poleg tega mora biti organizacija pozorna na možnost pridobitve dokumentacije, potrebne za namestitev in upravljanje varnostnega prehoda ter gradiv za dodatno usposabljanje skrbnikov (ISO, 2014, str. 20).

i) Tip izvedbe

Požarne pregrade se delijo glede na tip izvedbe. Prvi tip so požarne pregrade, ki so nameščene na namenski strojni napravi. Te naprave navadno sestavljajo utrjen operacijski sistem, nekatere pa vsebujejo tudi aplikacijsko specifično integrirano vezje, ki je namenjeno izvajanju določenih nalog, kot na primer izvajanju kriptografskih funkcij. Drug tip so požarne pregrade v obliki programske opreme. Te se delijo na tri tipe, tako imenovane osebne požarne pregrade, ki jih namestimo na osebne računalnike ter na namenske požarne pregrade, ki so nameščene na utrjen operacijski sistem ali v obliki navideznih naprav (ISO, 2014, str. 20).

j) Visoka razpoložljivost

Standard v tej točki priporoča, da organizacije vedno stremijo k uporabi sistemov ali arhitekture, ki omogoča visoko razpoložljivost. Večino varnostnih prehodov omogoča neki način postavitve sistema v visoki razpoložljivosti z uporabo tehnologije grozdov ali uporabo namenskih stikal, ki omogočajo izenačevanje obremenitve (ISO, 2014, str. 21).

k) Možnost integracije

Standard predlaga tudi iskanje rešitev, ki omogočajo tudi integracijo varnostnih mehanizmov drugih proizvajalcev, kot na primer IDS/IPS sistemov in protivirusnih programov. Rešitev lahko omogoča integracijo znotraj naprave ali preko aplikacijskih programskih vmesnikov (ISO, 2014, str. 21).

2.6 ISO/IEC 27033-5:2013

Peti del standarda, ISO/IEC 27033-5:2013, ki je bil izdan sredi leta 2013 in v celoti zamenjuje standard ISO/IEC 18028-5:2006, ima naziv Varovanje omrežnih povezav z uporabno navideznih zasebnih omrežij.

2.6.1 Obseg in struktura

V tem delu standard podaja smernice za izbor, izvedbo in spremljanje tehničnih kontrol, potrebnih za zagotavljanje varnosti povezav med omrežji in uporabniki z uporabo navideznih zasebnih omrežij. V prvem delu opisuje varnostne grožnje in zahteve, povezane z navideznimi zasebnimi omrežji v sledečih delih pa kontrole, tehnike snovanja navideznih zasebnih omrežij in smernice za izbor opreme (ISO, 2013c, str. 1-2).

2.6.2 Priporočila in zahteve

Navidezna zasebna omrežja (v nadaljevanju VPN omrežja) se uporabljajo za vzpostavitev varnih šifriranih podatkovnih kanalov med različnimi omrežji in omrežji ter uporabniki.

Uporabniku oziroma organizaciji morajo zagotavljati predvsem zaupnost in integriteto podatkov, ki se prenašajo preko omrežja, razpoložljivost ter preverjanje istovetnosti in avtorizacijo uporabnikov navideznega zasebnega omrežja (ISO, 2013c, str. 3).

Standard ločuje tipe VPN omrežij glede na arhitekturo in iz perspektive OSI referenčnega modela. Arhitekturno jih ločuje na povezave točka-točka in točka-oblak. V prvem primeru gre za povezovanje dveh končnih entitet, uporabnika in omrežja ali dveh omrežij. V drugem primeru gre za povezovanje uporabnika ali omrežja z omrežjem v oblaku, kot je na primer omrežje MPLS. Gledano iz perspektive OSI referenčnega omrežja, pa standard ločuje tipe navideznih zasebnih omrežij na omrežja na drugem nivoju, tretjem nivoju in sedmem nivoju. V prvem primeru omrežje podaljšuje drugi omrežni nivo preko navidezne zasebne povezave med dvema omrežjema ali uporabniki in omrežjem organizacije. V drugem primeru je povezava vzpostavljena na tretjem omrežnem nivoju, preko katerega lahko pakete do povezanih omrežij usmerjamo z različnimi usmerjevalnimi protokoli. V tretjem primeru pa gre za varno povezovanje aplikacij in uporabnikov z omrežjem organizacije z uporabo protokolov na sedmem OSI nivoju (ISO, 2013c, str. 3-4).

V nadaljevanju bom predstavil varnostne grožnje, kontrole, tehnike snovanja in smernice za izbor opreme, kot jih predlaga standard.

2.6.2.1 Varnostne grožnje

Standard v tej točki ugotavlja, da se bodo organizacije v prihodnosti spopadale z vedno bolj naprednimi napadi na njihovo informacijsko infrastrukturo. Pri uporabi VPN omrežij deli napade na vdore in napade onemogočanja storitev. Izvor obeh oblik napadov so lahko notranja omrežja organizacije, VPN omrežja, javna omrežja ali jedrna omrežja ponudnika storitev. Proti vdorom se lahko organizacija zavaruje z omejevanjem prometa iz vseh prej naštetih izvornih točk proti svojim omrežjem ali v posamezna varnostna območja znotraj omrežja. Težje se organizacije zaščitijo pred napadi onemogočanja in porazdeljenimi napadi onemogočanja. Kot najboljšo zaščito pred tovrstnimi napadi izpostavlja dobro snovanje navideznih zasebnih omrežij. Pri tem mora organizacija paziti, da prepreči uhajanje informacij o interni strukturi omrežja, prepreči ponarejanje oznak v MPLS omrežjih in zagotovi odpornost na napade onemogočanja in porazdeljenega onemogočanja storitev ter napade z izrabo neavtoriziranega dostopa (ISO, 2013c, str. 4).

2.6.2.2 Varnostne zahteve

Sistemi navideznih zasebnih omrežij morajo zagotavljati zaupnost in celovitost podatkov, ki se prenašajo med končnima točkama povezave, razpoložljivost omrežne infrastrukture in končnih točk ter preverjanje istovetnosti in overjanje dostopa vseh uporabnikov ter skrbnikov (ISO, 2013c, str. 5).

Zaupnost podatkov, ki se prenašajo preko VPN omrežja, je ena najbolj pomembnih varnostnih zahtev. Odvisna je od verjetnosti, da nekdo podatke na poti skozi omrežja prestreže, zato je treba podatke šifrirati bodisi med prenosom bodisi pred začetkom prenosa na njihovem izvoru. Poleg zaščite podatkov med prenosom pa standard opozarja tudi na pomembnost zagotavljanja visoke varnosti na končnih točkah vzpostavljenega tunela. Tu je treba z izklopom usmerjanja in uporabo filtriranja paketov ali požarnimi pregradami preprečiti, da bi se preko navideznega zasebnega omrežja prenašal nenadzorovan promet (ISO, 2013c, str. 5-6).

Druga pomembna varnostna zahteva je zagotavljanje celovitosti podatkov. Zagotoviti je treba preverjanje integritete podatkov, ki se prenašajo preko navideznega zasebnega omrežja. To lahko zagotovimo na sistemu navideznih zasebnih omrežij ali na izvorni in ponorni strani podatkov. Standard pri tem predlaga uporabo kod za overitev sporočila, kod za preverjanje sporočila in mehanizme za preprečevanje ponavljanja (ISO, 2013c, str. 6).

Ker navadno navidezna zasebna omrežja dovolijo vzpostavljanje komunikacije s sistemi v omrežjih znotraj organizacije, sta pri tem pomembni tudi verodostojnost in overjanje. Sistemi za vzpostavljanje navideznih zasebnih omrežij morajo verodostojnost zagotavljati s preverjanjem verodostojnosti druge točke navideznega zasebnega omrežja, overjanje pa z uporabo seznamov za kontrolo dostopa, kjer so vpisane končne točke navideznih zasebnih omrežij in posledično dovoljujejo vzpostavitev komunikacije le med temi točkami (ISO, 2013c, str. 6).

Poleg vseh prej naštetih varnostnih zahtev, ki zagotavljajo zaupanje v navidezna zasebna omrežja, pa je zelo pomembna tudi razpoložljivost. Ta je zelo odvisna od omrežja, preko katerega je neko navidezno zasebno omrežje vzpostavljeno, ter od izpostavljenosti oziroma dovzetnosti rešitve na napade onemogočanja in porazdeljenega onemogočanja storitev. Rešitev mora zagotavljati zadovoljivo stopnjo odpornosti na napade ter izpade delov omrežja z vzpostavitvijo alternativnih povezav (ISO, 2013c, str. 6).

2.6.2.3 Varnostne kontrole

Rešitve VPN omrežij uporabljajo različne tipe tuneliranja podatkov med končnimi točkami, zagotoviti pa morajo tudi šifriranje tunelov oziroma podatkov v tunelih, kar sicer dvigne stopnjo varnosti prenesenih podatkov, še vedno pa lahko napadalec s prestrezanjem paketov na omrežju vidi končni točki vzpostavljenega tunela. Organizacija mora z vzpostavitvijo varnostnih kontrol na končnih točkah tunelov zagotoviti dovolj visoko stopnjo varnosti, da bo celotna rešitev skladna z varnostno politiko organizacije ter sprejemljivimi stopnjami tveganj. Enako je treba zagotoviti tudi v primerih, ko organizacija od ponudnikov najema ločeno infrastrukturo za vzpostavitev povezav med različnimi lokacijami. Takšne povezave so sicer varnejše kot uporaba javnih omrežij, a so še vedno odvisne od varnosti omrežja ponudnika najete povezave. Standard zato predlaga uporabo šifriranja in vzpostavitve visoke varnosti končnih točk tudi v primeru najetih povezav (ISO, 2013c, str. 6-7).

2.6.2.4 Tehnike snovanja

VPN omrežje povezuje dve končni točki preko obstoječih fizičnih omrežij in povezav z uporabo različnih protokolov tuneliranja in šifriranja podatkov. Stopnja varnosti se torej razlikuje že glede na omrežje oziroma povezavo, preko katere je vzpostavljeno navidezno zasebno omrežje. Pri povezovanju preko javnih omrežij je stopnja varnostni in zanesljivosti najnižja, višja je pri povezovanju preko omrežja ponudnika storitev, najvišja pa pri vzpostavljanju navideznega zasebnega omrežja znotraj omrežja organizacije. Največkrat se za izvedbo navideznega zasebnega omrežja uporablja tuneliranje podatkov, saj je takšna povezava transparentna za transportno omrežje in omogoča uporabo na enak način, kot se uporabljajo fizične povezave. Tuneli med dvema točkama so lahko vzpostavljeni z navideznimi vodi, uporabo labelne komutacije ter ovijanjem protokola. V vseh primerih je treba zaupnost zagotoviti z uporabo kriptografskih metod in tehnik (ISO, 2013c, str. 7-8).

Standard, kot v mnogih predhodnih točkah, pri uporabi VPN omrežij opozarja na skladnost z regulatornimi in zakonskimi zahtevami v vseh državah, ker se tovrstne povezave začenjajo ali zaključujejo. Pri tem mora organizacija paziti na zahteve glede varovanja podatkov, uporabe kriptografskih metod in tehnologij ter upravljanje z operacijskimi tveganji. Poleg regulatornih in zakonskih zahtev mora organizacija detajlno preučiti tudi poslovne zahteve. Organizacija mora analizirati vsa tveganja, povezana z VPN omrežji, identificirati področja kontrole ter skladno s poslovnimi zahtevami načrtovati, izvesti in vzdrževati varnostne kontrole. Pri tem daje standard velik poudarek na ozaveščenost uporabnikov in skrbnikov o tveganjih, povezanih z uporabo navideznih zasebnih omrežij (ISO, 2013c, str. 8).

Pri snovanju VPN omrežij je pomembno preučiti tudi različne arhitekturne oblike. Za zagotavljanje skladnosti z vsemi prej napisanimi varnostnimi zahtevami je treba zagotoviti varnost celotnega sistema VPN omrežij. Primerno je treba zaščititi povezave in vse končne točke povezav, ki so lahko varnostni prehodi, strežniki, različne naprave končnih uporabnikov itd. Te morajo biti zaščitene pred nepooblaščenim fizičnim dostopom in oddaljenim nepooblaščenim dostopom, zaščitene morajo biti tudi pred raznovrstnimi virusi in škodljivo programsko opremo. Organizacija mora zagotoviti tudi ustrezno upravljanje tehničnih ranljivosti vseh naprav ter skrbeti za ozaveščenost uporabnikov in skrbnikov. Poleg same varnosti končnih točk je treba zagotoviti tudi varnost podatkov pri vstopu in izstopu iz končne točke proti omrežju organizacije. Preko končne točke na ponorni strani povezave so navadno dosegljivi notranji sistemi organizacije, kar pomeni, da je njihova varnost odvisna od varnosti te točke. Standard priporoča, da so končne točke nameščene na napravah v posebnem delu omrežja, kjer nam varnostni prehodi omogočajo filtriranje prometa, morebitno pregledovanje vsebine za vsebnost virusov in škodljive programske kode ter pregledovanje prometa za morebitne napade s sistemi za zaznavanje in preprečevanje vdorov. Velik del varnosti predstavlja tudi način tuneliranja podatkov. Standard priporoča usmerjanje vseh podatkovnih tokov preko vzpostavljene povezave, saj sta pri uporabi razcepljenih tunelov končna točka in omrežje organizacije izpostavljena večjim varnostnim tveganjem (ISO, 2013c, str. 8-11).

Poleg prej opisanih kontrol pa mora rešitev omogočati še dve ključni zadevi. Overjanje in beleženje dogodkov. Overjanje je treba izvajati na dveh nivojih. Na prvem nivoju morajo končne točke zagotavljati mehanizme za overjanje naprav, ki želijo vzpostaviti navidezno zasebno omrežje. Tu ostajata dve možnosti, in sicer overitev s skupnim ključem in overitev z uporabo digitalnih potrdil, ki ju lahko po potrebi kombiniramo tudi s seznami za kontrolo dostopov. Na drugem nivoju morajo končne točke zagotavljati overjanje uporabnikov z uporabo uporabniških imen in gesel, digitalnih potrdil ali gesel za enkratno uporabo. Še zadnja ključna zadeva, ki jo standard predpisuje pri tehnikah snovanja, pa je zagotavljanje beleženja dogodkov za potrebe revizije dostopov, zagotavljanja sledljivosti in nadzora nad navideznimi zasebnimi omrežji (ISO, 2013c, str. 11).

2.6.2.5 Tehnični dejavniki navideznih zasebnih omrežij

Pri vzpostavitvi VPN omrežij so pomembni tudi določeni tehnični dejavniki. Standard v tej točki izpostavlja izbor protokola nosilca, dilemo pri uporabi strojnih in programskih rešitev, upravljanje končnih točk ter nadzorovanje varnosti navideznega zasebnega omrežja. Upravljanje zajema nastavitev omrežja in protokolnih vrat glede na varnostne zahteve in kontrole, namestitev digitalnih potrdil in vzpostavitev nadzora nad navideznim zasebnim omrežjem. Nadzor je ključen za zagotavljanje omrežnih varnostnih kontrol, saj VPN omrežja na neki način širijo meje omrežja organizacije na oddaljene lokacije, največkrat v nenadzorovanem delu javnega omrežja. Zagotoviti je treba hranjenje zapisov za presojo, ki skrbnikom omrežnih sistemov omogočajo zaznavo in odziv na morebitne varnostne incidente. Standard poleg tega priporoča tudi namestitev sistemov za zaznavanje vdorov in vzpostavitev alarmiranja skrbnikov ob pojavu varnostnih incidentov, rutinsko pregledovanje sistemov in vzpostavitev sistematičnega šolanja uporabnikov z namenom, da bi znali zaznati varnostne incidente in o njih poročati odgovornim osebam (ISO, 2013c, str. 11-12).

2.6.2.6 Smernice za izbor opreme

Smernice, ki jih standard priporoča za izbor opreme, se navezujejo na transportni protokol in naprave. Organizacija mora, glede na poslovne zahteve, zahteve po medsebojni obratovalnosti z drugimi rešitvami, trenutnim dojemanjem trga ter analizo znanih slabosti protokola oziroma odpornosti protokola na različne grožnje, izbrati želeni transportni protokol za izvedbo navideznih zasebnih omrežij in na podlagi tega primerno rešitev. Standard kot drugo smernico predlaga izbor namenskih naprav, saj prinašajo številne prednosti, kot so večja varnost, lažje upravljanje, različne možnosti overjanja itd. (ISO, 2013c, str. 12-13).

V nadaljevanju magistrskega dela bom analiziral tipe in tehnike sodobnih napadov na omrežja z namenom preučitve učinkovitosti varnostnih priporočil in zahtev standarda pri varovanju omrežij pred njimi.

3 TIPI IN TEHNIKE SODOBNIH NAPADOV NA OMREŽJA

Poznavanje različnih tipov in tehnik napadov je osnova za izgradnjo varnega omrežja in informacijskega sistema. S časom se napadi razvijajo in spreminjajo kot odgovor razvoju sistemov in tehnik, ki nas pred njimi obranijo. V nadaljevanju bom opisal tipe napadov, sodobne tehnike njihovega zaznavanja in preprečevanja, analiziral nekaj najbolj odmevnih napadov zadnjega časa in naredil pregled najbolj uporabljanih orodij za izvajanje napadov.

3.1 Tipi in motivi napadov na omrežja

Izrabljanje različnih ranljivosti v sistemih, storitvah in aplikacijah, neposredno ali s pomočjo socialnega inženiringa, so stalnica napadov na različne informacijske in komunikacijske sisteme. Izbrani način napada je odvisen od napadalca in ciljnega sistema, mnogokrat pa je odvisen tudi od motiva. Če želi napadalec onesposobiti neko spletno storitev, bo redko posegel po naprednih in težkih tehnikah pridobitve dostopa do infrastrukture, temveč bo na ciljni sistem izvedel napad onemogočanja ali porazdeljeni napad onemogočanja storitve. Nasprotno bo napadalec, ki želi dolgoročno pridobivati zaupne podatke organizacije, posegel po tipih napadov, s katerimi bo njegov vdor dalj časa ostal skrit različnim varnostnim sistemom in skrbnikom ciljnih sistemov.

3.1.1 Motivi napadov

Motivi za napade se v grobem delijo na finančne, vohunjenje, pridobivanje veščin, slava, zabava, hektivizem, terorizem in (kibernetska) vojna (Andress & Winterfeld, 2014; Shakarian, Shakarian & Ruef, 2013). Andress in Winterfeld (2014, str. 28-31) delita napadalce na notranje in zunanje. Glede na zadnje poročilo korporacije Verizon (2015, str. 4-5) o uspešnih napadih v letu 2014, je okoli 20 % napadov izvedenih znotraj organizacije, okoli 1 % izvedejo partnerji, preostalo pa zunanji napadalci. Notranje napadalce Andress in Winterfeld (2014, str. 28-31) delita na nezadovoljne zaposlene, finančno motivirane zaposlene in tiste, ki varnostni incidenti in posledično škodo organizaciji povzročijo nenamerno. Zunanje napadalce delita na organizirane kriminalne združbe, hektiviste in novince. Motivi organiziranih finančnih združb so največkrat finančni, mnogokrat pa napadajo uporabnike in informacijske sisteme izven lastne države. Hektivisti so navadno politično, kulturno, religiozno, nacionalno ter teroristično motivirani posamezniki ali skupine. Novinci, ki za napade uporabljajo predvsem orodja dostopna preko interneta in ne posedujejo mnogo znanja o vdorih v sisteme, imajo različne motive za napade, največkrat pa so to pridobivanje izkušenj in slave, na podlagi katere si lahko prislužijo mesto v večjih hekerskih skupinah. Tako imenovani hekerji in skupine hekerjev se delijo hekerje, ki vdirajo v sisteme z namenom ugotavljanja ranljivosti in jih navadno za to najamejo različne organizacije, hekerje, ki svoje znanje uporabljajo za nelegalne aktivnosti in hekerje, ki delajo po svoji vesti in včasih zaidejo tudi na nelegalno stran, če menijo, da bo to dolgoročno pomagalo pri zagotavljanju splošne informacijske varnosti (Andress & Winterfeld, 2014, str. 28-30). Največkrat pa so pravi motivi kriminalnih združb zakriti in jih je težko

prepoznati. Tudi v primerih, ko napadalec ali neka skupina prizna napad, je lahko za tem več motivov, kot sta finančna motivacija in politična motivacija (Shakarian et al., 2013, str. 1-8). V svojem poročilu Verizon (2015) ugotavlja, da je bila v letu 2014 v 70 % napadov, kjer je bil motiv poznan, žrtev primarnega napada le odskočna deska za izvajanje napada na drugo žrtev. Pri tem so hekerji primarni napad največkrat izvedli z izrabo ranljivosti na žrtvinem sistemu ali socialnim inženiringom v obliki elektronske pošte, za sekundarni napad pa so uporabljali različne tipe napadov. Motiv prvega napada je bil le pridobitev dostopa do sistemov, s pomočjo katerih so napadalci pri izvajanju nadaljnjih napadov nato zakrili svojo identiteto (Verizon, 2015).

3.1.2 Tipi napadov

Napade delimo na aktivne in pasivne. Pri aktivnih napadih napadalec z izvajanjem različnih ukazov na sistemu vpliva na njegovo delovanje, pasivni napadi pa se uporabljajo bolj za namene zbiranja podatkov (Pawar & Anuradha, 2015, str. 504-505).

Pasivni napadi se izvajajo na omrežnem nivoju. V to kategorijo spadajo spremljanje prometa, prisluškovanje in analiza prometa. Spremljanje prometa in prisluškovanje napadalcu omogočata vpogled v podatkovni tok preko ožičenih in brezžičnih omrežij. Z analizo pridobljenega prometa lahko napadalec iz podatkov izlušči različne informacije zaupne narave, kot so gesla, žetoni overitvenih algoritmov, uporabljani omrežni in usmerjevalni protokoli, tipi izvornih in ponornih sistemov, aplikacij na omrežju itd. Pasivni napadi so največkrat faza zbiranja informacij, ki jih napadalci kasneje uporabijo pri aktivnem napadu bodisi na omrežno opremo bodisi na ostale informacijske sisteme organizacije (Daya, 2013; Pawar & Anuradha, 2015).

Aktivni napadi se po namenu delijo v dve skupini, in sicer na onemogočanje storitev ter napade z namenom pridobivanja dostopov. Onemogočanje omrežnih storitev lahko napadalci dosežejo na več načinov. Največkrat napad izvedejo z ustvarjanjem velikega števila zahtev za določeno storitev, kar na ciljnem sistemu povzroči pomanjkanje virov za izvajanje storitve in posledično nedosegljivost storitve za njene uporabnike. Druga možnost je ustvarjanje velikega števila velikih paketov, s katerimi zapolnijo propustnost neke povezave in s tem prekinejo komunikacijo med omrežjema, ki ju ta povezava povezuje. Če ima napadalec dostop do sistema v omrežju, pa lahko onemogoči storitev tudi s preprečevanjem posredovanja paketov na omrežni napravi, izklopom vmesnikov na omrežni napravi, izklopom omrežne naprave ali s spreminjanjem nastavitev usmerjanja. S spremembo usmerjanja na omrežni napravi ali v celotnem omrežju lahko napadalec usmeri promet tudi preko njegovega sistema, na katerem lahko izvaja različne pasivne napade ali pa v podatkovni tok tudi aktivno posega. Preusmeritev lahko izvede na različne načine. Napad s ponarejanjem omogoča, da napadalec ponaredi sporočila usmerjevalnega protokola in na ta način preusmeri pakete na drug naslov. Napad s sleparjenjem s podatki o identiteti napadalcu omogoči ponarejanje identitete enega od usmerjevalnikov znotraj omrežja in tako preusmeri promet preko svojega sistema. Če ima napadalec dostop do enega od usmerjevalnikov, lahko na njem spremeni usmerjevalno tabelo in

tako na drugo točko preusmeri ves promet, ki potuje preko tega usmerjevalnika. Še bolj napreden je napad s tuneliranjem, pri katerem lahko napadalec vzpostavi tunel med usmerjevalnikom znotraj omrežja organizacije in sistemom izven omrežja organizacije in preko njega preusmeri ves promet organizacije. Seveda lahko napadalec z vsemi naštetimi in podobnimi napadi vpliva tudi na delovanje omrežja oziroma posredovanje paketov, pogoj pri tem pa je, da ima napadalec dostop do naprave ali vozlišča znotraj omrežja organizacije. Do dostopa lahko napadalci pridejo na več načinov. Največkrat uporabijo socialni inženiring, s katerim uporabnika ali njegovo napravo prelisičijo, da jim dostop omogoči. Druga možnost so v drugem odstavku opisani pasivni napadi, s pomočjo katerih napadalec pridobi poverilnice za dostop do vozlišča. Obstaja pa tudi vrsta aktivnih napadov na vozlišča, ki na različne načine napadalcu omogočijo dostop do vozlišča. Pri napadu s ponarejanjem IP paketov napadalec pripravi IP pakete, ki vsebujejo nabor ukazov s katerimi namerava spremeniti delovanje vozlišča. Pri ustvarjanju paketov za njihov izvorni naslov uporabi IP naslov nekega sistema, ki mu napadeno vozlišče zaupa. S pošiljanjem tako narejenih paketov spremeni delovanje vozlišča v taki meri, da mu vozlišče omogoči dostop. Za dostop do ostalih vozlišč lahko nato uporabi napad s ponavljanjem overitvenih paketov med skrbnikovo postajo in ciljnim vozliščem ter s tem pridobi uporabniško ime in geslo za dostop do ciljnih vozlišč (Daya, 2013; Pawar & Anuradha, 2015). Izvedba naštetih napadov je dokaj zapletena, saj od napadalca zahtevajo veliko znanja, predvsem, če ta ne želi, da bi kdo njegovo početje zaznal.

Včasih pa se napadalcem nasmehne tudi sreča oziroma nevestno obnašanje proizvajalcev omrežne opreme. V letih 2013 in 2014 so strokovnjaki za informacijsko varnost odkrili enostaven način vdora v različna omrežja po celem svetu. Eckstein (2014, str. 2-4) v svojem poročilu opisuje, kako so raziskovalci v različnih omrežnih napravah odkrili stranska vrata, ki so jih na programsko opremo naprav namestili kar proizvajalci sami. Vdelana stranska vrata omogočajo dostop do omrežne naprave s skrbniškimi pravicami, kar seveda uporabljajo tudi hekerji. To dodatno podpre priporočilo četrtega in petega dela standarda ISO/IEC 27033, da je treba pri izboru opreme izvesti analizo znanih ranljivosti (ISO, 2013c, 2014). S kombinacijo pasivnih in aktivnih napadov pa lahko napadalci izrabljajo tudi različne pomanjkljivosti v šifrirnih protokolih, ki so opisane v točki 3.3.

Poleg prej opisanih aktivnih in pasivnih napadov na omrežne in informacijske sisteme pa napadalcem dostop do omrežja in informacijskih sistemov mnogokrat omogočijo neozaveščeni zaposleni znotraj organizacije. Te, kot žrtve raznih prevar in nepazljivosti, nevede svoje delovne postaje okužijo z različnimi virusi, črvi in trojanskimi konji, mnogokrat pa so tudi žrtve napadov z ribarjenjem in napadalcem v dobri veri posredujejo podatke za dostop do omrežnih ali informacijskih sistemov organizacije (Andress & Winterfeld, 2014; Daya, 2013; Pawar & Anuradha, 2015). Nove tehnike napadov spremljajo tudi nove tehnične rešitve njihovega preprečevanja, je pa kljub temu napadov iz leta v leto več (NIST, 2015). Poleg pojavljanja novih tehnik napadov se hitro razvijajo tudi tehnike izogibanja zaznave napadov, ki jih bom predstavil v naslednjem poglavju.

3.2 Najnovejše tehnike izogibanja zaznave napadov

Osnovne tehnike izogibanja zaznave napadov in vdorov zadnja leta sicer ostajajo približno enake, napadalci pa jih uspešno kombinirajo v nove vektorje napadov, s katerimi poskušajo svoje napade skriti pred sistemi za zaznavanje vdorov.

3.2.1 Osnovne tehnike izogibanja zaznave napadov

Osnovne tehnike izogibanja zaznave napadov so tiste, ki se uporabljajo predvsem za izogibanje zaznave na sistemih za zaznavanje (v nadaljevanju IDS sistemi) in preprečevanje vdorov (v nadaljevanju IPS sistemi). Ti sistemi v aktivni ali pasivni namestitvi v omrežje preverjajo podatkovni tok in v paketih iščejo vzorce znanih napadov. Vzorci so lahko na sistemu v obliki podpisov, podobno kot pri protivirusnih programih, ali pa jih sistem ustvarja samodejno glede na dolgoročno vzorčenje prometa in anomalij v prometu. Z razvojem programske in strojne opreme so se razvile tudi metode pregledovanja paketov, vendar določene šibke točke sistemov zaradi različnih značilnosti v transportnih protokolih in stalnega razvoja zlonamerne programske opreme napadalcev, še vedno ostajajo. Največja težava pri IDS/IPS sistemih so napačno pozitivne in napačno negativne zaznave napadov. Napačno pozitivna zaznava napada pomeni, da je sistem neki legitimen paket ali podatkovni tok zaznal kot napad. Napačno negativna zaznava pa je nasprotje tega, torej da sistem ni zaznal nekega napada, ker v paketu ali podatkovnem toku ni našel vzorca, ki bi na napad nakazoval. Slaba stran napačno negativnih zaznav je, da sistem napada ne zazna in posledično tudi ne prepreči oziroma o njem ne obvesti odgovornih oseb. Zaradi te napake lahko napadalec uspešno izvede vdor v informacijski sistem organizacije in tega organizacija ne zazna. Kljub temu, da na prvi pogled napačno pozitivne zaznave nimajo močnega vpliva na varnost komunikacij, pa ni tako. V primeru aktivno nameščenega IPS sistema lahko ta ob napačni zaznavi blokira legitimni promet in s tem izvede prekinitev dostopa do storitve ali sistema, kar lahko negativno vpliva na poslovanje organizacije. V primeru pasivno nameščenega IDS sistema, ki ob zaznavi napada le obvešča odgovorne osebe in aktivno ne posega v promet, pa bo ob velikem številu napačno zaznanih napadov zaupanje v ta sistem omajano, kar lahko pripelje tudi do neupoštevanja alarmov o napadih, ki jih ta sistem ustvarja. Da bi se ognili napačnim zaznavam napadov, morajo skrbniki IDS/IPS sistemov izvajati ročno popravljanje nastavitev, s čimer pa lahko vplivajo tudi na napačno negativno zaznavo napadov (Cheng, Lin, Lai & Lin, 2012; Del Carlo, 2003; Dela Torre & Sioting, 2013).

Poleg prej opisanih težav pa so IDS/IPS sistemi predvsem zaradi omejitev z viri in zahtevami po vedno večji hitrosti prenosa podatkov in vedno manjših zakasnitvah, ranljivi za različne načine izogibanja zaznave napadov. Najbolj agresivna oblika izogibanja zaznave napada je napad na onemogočanje storitve IDS/IPS sistema. Pri IDS sistemih je tak napad enostavneje izvesti kot pri IPS sistemih, ker IDS sistemi ne posegajo aktivno v promet in napadalcu ni treba paziti, da bi z napadom na IPS sistem onemogočil tudi dostop do njegovega cilja. IDS sistemi so v omrežje največkrat priključeni pasivno, torej preko vmesnika za zrcaljenje prometa.

Poznamo tri različne tipe napadov, s katerimi je moč onemogočiti storitev zaznavanja napadov.

Prvi je preplavljanje IDS/IPS sistema v kombinaciji s sleparjenjem z naslovi. S tem napadalec doseže, da sistem zaznava napade iz veliko različnih izvornih naslovov, zaradi česar odgovorne osebe ne morejo določiti, kateri naslov je tisti, ki napad resnično izvaja. Druga možnost je preplavljanje IDS/IPS sistema s posebej narejenimi paketi, ki sprožijo napačno zaznavo napada. Cilj takšnega napada je, da varnostni inženirji začasno izklopijo alarmiranje in blokiranje prometa, takrat pa napadalec sproži pravi napad in z njim pridobi dostop do ciljnega sistema. Tretji tip napada je izčrpavanje virov. Pri takšnem napadu napadalci z veliko količino legitimnega prometa porabijo vse procesorske, pomnilniške ali pretočne vire IDS/IPS sistema. Večina IPS teh sistemov je namreč privzeto nastavljenih na posredovanje paketov brez pregledovanja v primeru preobremenitve. Ob preobremenitvi napadalci v legitimni promet skrijejo napad in izvedejo vdor v končni sistem. Za izvajanje naštetih napadov morajo imeti napadalci veliko znanja, poleg tega pa morajo dobro poznati varnostno arhitekturo omrežja, ki ga napadajo. IDS/IPS sisteme morajo ohromiti na način, da omrežje in cilj, ki ga napadajo, še vedno ostanejo dosegljivi in dovzetni za napad (Cheng et al., 2012; Del Carlo, 2003; Ptacek & Newsham, 1998).

Druga oblika izogibanja zaznave napadov je napad z vstavljanjem. Pri tem napadu napadalec v podatkovni tok vstavi pakete, za katere ve, da jih bo napadeni sistem zavrnil, IDS/IPS sistem pa obravnaval kot del podatkovnega toka. Tako lahko v podatkovni tok skrije mašila, ki podatkovni tok pri pregledovanju na IDS/IPS sistemu spremenijo do te mere, da napadov sistem ne zazna. Ko pridejo vsi paketi do napadenega sistema, ta zavrne pakete, ki so delovali kot mašilo, sestavljeni podatkovni tok pa uspešno izvede vdor v sistem (Cheng et al., 2012; Ptacek & Newsham, 1998).

Podobni prejšnjemu napadu so tudi napadi z drobljenjem paketov. Drobljenje paketov je funkcionalnost TCP/IP protokola, s katero lahko sistem pakete, ki so za neko omrežje preveliki, razdrobi na več manjših paketov, ki jih prejemnik spet sestavi v prvotni paket. Da bi IDS/IPS sistem lahko zaznal napad, mora vse drobce paketa med pregledovanjem prejeti, sestaviti v končni paket in ga primerjati s podpisi napadov. Vsi novejši IDS/IPS sistemi to funkcionalnost sicer omogočajo, vendar jih lahko napadalec z manipulacijo drobcev na različne načine prelisiči. Ker sestavljanje drobcev zahteva procesorsko in pomnilniško moč, lahko napadalec z velikim številom drobcev izvede napad onemogočanja storitve sestavljanja paketov in tako IDS/IPS sistem pakete posreduje cilju brez pregledovanja. Poleg uporabe velikega števila drobcev lahko napadalec pošilja drobce v tako velikih časovnih razmikih, da jih končni sistem še sprejme, IDS/IPS sistem pa zaradi časovnih omejitev opusti pregledovanje podatkovnega toka in pregleda ter posreduje vsak posamični drobec. Druga možnost je drobljenje paketov z vstavljanjem mašil na podoben način, kot je to opisano v prejšnjem odstavku. Tretja možnost je prekrivanje drobcev, pri čemer napadalec z manipuliranjem podatkov v IP paketu ob sestavljanju paketa prekrije del predhodnega ali sledečega drobca. Te napade omogočajo različne izvedbe TCP/IP protokolnega sklada na različnih sistemih, kjer določeni sistemi

prekrivajo predhodni drobec, drugi naslednji drobec, tretji pa takšne pakete zavržejo. Če torej IDS/IPS uporablja drugačno prekrivanje drobcev kot ciljni sistem, lahko napadalec to izkoristi in izvede napad brez zaznave (Cheng et al., 2012; Del Carlo, 2003; Ptacek & Newsham, 1998).

Četrta oblika napada za izogibanje zaznavi so razne metode zakrivanja. Nekatere metode izrabljajo podobno problematiko kot je opisana v prejšnjem odstavku, in sicer različno interpretacijo podatkov na IDS/IPS sistemu in ciljnem sistemu, druge pa poskušajo zakriti napad s simuliranjem različnih aplikacijskih protokolov, kot na primer razne protokole za sporočanje, HTTP protokol in podobno. Pri metodi zakrivanja napadalci določen del podatkov zamaskirajo z uporabo različnih semantično ekvivalentnih znakov. IDS/IPS sistem mora torej zapis dekodirati točno na tak način, kot bi ga dekodiral napadeni sistem. Ker je takšnih kodiranj veliko, morajo IDS/IPS sistemi vsak paket pregledati z različnimi dekodirniki, kar se seveda zopet odraža v večji porabi virov, večjih zakasnitvah pri posredovanju paketov in posledično tudi manjši hitrosti posredovanja paketov. Drug način, ki ga vedno pogosteje uporabljajo današnji napadalci, pa je tako imenovano legitimiziranje prometa. Pakete, ki vsebujejo neke vrste napad in ga IDS/IPS sistemi normalno zaznajo, maskirano v različne protokole drugih aplikacij, s čimer simulirajo legitimni promet in se s tem dokaj učinkovito izognejo zaznavi napada ali prenosa zaupnih podatkov iz omrežja organizacije. To največkrat izrabljajo v primerih, ko imajo do nekega sistema že dostop in želijo na ta sistem preko IDS/IPS sistema prenesti novo zlonamerno programsko kodo. Tovrstna izogibanja zaznavanja napadov je najtežje prepoznati, saj je v mnogih primerih zelo težko ločiti legitimni promet od nelegitimnega, podpisi tovrstnih napadov pa so dokaj neučinkoviti in mnogokrat prožijo veliko lažno pozitivnih alarmov (Cheng et al., 2012; Del Carlo, 2003, str. 4-5; Dela Torre & Sioting, 2013).

Zadnja vrsta izogibanja, ki se skozi leta zelo uspešno uporablja, pa je uporaba šifriranja. Pred časom je bilo to tehniko sicer veliko lažje uporabljati, saj IDS/IPS sistemi takrat še niso znali pregledovati šifriranega prometa. Že uporaba SSL šifriranja HTTP povezave je pomenila uspešno izogibanje zaznavi, saj so navadno IDS/IPS sistemi šifriran promet le posredovali proti cilju. Danes to IDS/IPS sistemi rešujejo z uporabo t. i. napada vmesnega človeka. IDS/IPS sistem poskus vzpostavitve šifrirane seje med izvornim in ponornim sistemom prestreže in sejo odjemalca s simuliranjem strežnika zaključi na prejemnem vmesniku, nato pa kot odjemalec vzpostavi sejo proti ponornemu sistemu. Dešifrirani promet nato posreduje različnim varnostnim komponentam IDS/IPS sistema. Pogoj, da uporabniki tega ne zaznajo, je uporaba zaupanja vrednega certifikatskega organa na IDS/IPS napravi, česar pa znotraj organizacije ni težko vzpostaviti. Seveda pa takšne analize zaradi določenih omejitev in varnostnih elementov šifrirnega protokola ni mogoče vedno izvajati. Ena takšnih omejitev je relativno slaba podpora različnim šifrirnim protokolom na strani IDS/IPS sistemov. Večina novejših IDS/IPS sistemov omogoča dešifriranje HTTP SSL sej, več težav pa imajo proizvajalci teh sistemov že pri dešifriranju IPSEC protokola. Napadalec lahko torej za svoje zlonamerne podvige uporabi protokol, ki ga IDS/IPS sistem ne zna dešifrirati. Druga težava nastane pri uporabi digitalnih potrdil za preverjanje istovetnosti odjemalcev. SSL protokol pri takšni uporabi uporablja

različne mehanizme za zagotavljanje celovitosti in takšne seje pri prej opisanem dešifriranju ni mogoče vzpostaviti. Tretja težava pa je zopet vezana na vire IDS/IPS sistema. Dešifriranje in ponovno šifriranje podatkovnih sej zahteva določene vire, ki pa jih IDS/IPS sistemi nimajo neomejeno, kar sisteme zopet izpostavi različnim oblikam napadov onemogočanja storitve (Cheng et al., 2012; Del Carlo, 2003; Dela Torre & Sioting, 2013).

3.2.2 Napredne tehnike izogibanja zaznave napadov

V zadnjih nekaj letih se v zvezi z informacijsko varnostjo pojavljata dva izraza, in sicer napredne tehnike izogibanja in napredne trajne grožnje. Napredne tehnike izogibanja so večinoma le kombinacija več različnih osnovnih tehnik izogibanja zaznave napadov. Napadalci izberejo kombinacijo tehnik, ki delujejo na več različnih nivojih OSI modela in tako napad skrijejo na različne nivoje. Ker IDS/IPS sistemi zaradi zahtev po hitrosti in propustnosti večinoma pregledujejo vsak sloj posebej, tovrstnega napada ne zaznajo (Dela Torre & Sioting, 2013; Niemi, 2013). Vdori, ki ostanejo skriti različnim varnostnim sistemom skozi daljše časovno obdobje, spadajo pod tako imenovane napredne trajne grožnje. Stroka si sicer glede prave definicije naprednih trajnih groženj še ni edina (ISACA, 2014, str. 6), največkrat pa se uporablja definicija Ameriškega nacionalnega inštituta za standarde in tehnologijo (v nadaljevanju NIST) (NIST, 2013, priloga B, str.1), ki definira napredno trajno grožnjo kot »nasprotna stran, ki ima visoko raven strokovnega znanja in znatna sredstva, ki omogočajo ustvarjanje priložnosti za dosego svojih ciljev s pomočjo različnih vektorjev napadov (kot na primer, kibernetični, fizični in napadi s prevaro). Ti cilji običajno vključujejo vzpostavitev in razširitev opore znotraj informacijske infrastrukture organizacij za namene pridobivanja informacij, spodkopavanja ali oviranja kritičnih poslovnih procesov programa ali organizacije; ali priprave na izvajanje teh ciljev v prihodnosti. Napredne trajne grožnje: (i) zasledujejo svoje cilje v daljšem časovnem obdobju; (ii) se prilagajo prizadevanjem varnostnemu osebju, da bi jih preprečili; in (iii) so odločne, da ohranijo raven interakcije potrebne za izvajanje svojih ciljev.« Pri tem ne gre torej za neke vrste zlonamerno programsko opremo, temveč za napadalca oziroma kriminalno združbo, ki ima dolgoročni cilj dostopati do zaupnih podatkov ali škoditi poslovnim procesom ciljne organizacije. Ta cilj dosega z naprednimi tehnikami izogibanja zaznave napadov in vdorov, ki temeljijo predvsem na namensko napisani zlonamerni programski kodi, ki izkorišča javnosti še neznane ranljivosti v različnih sistemih, programski opremi in storitvah (Gold, 2011; ISACA, 2014; McAfee, 2015).

V nadaljevanju bom opisal nekaj najbolj odmevnih ranljivosti in napadov zadnjega časa.

3.3 Pregled zadnjih najbolj odmevnih ranljivosti in napadov

V letu 2014 smo bili priča največjemu številu različnih tipov ranljivosti do sedaj. NIST (2015) je zabeležil kar 7.937 ranljivosti, vplivale pa so tako na varnost omrežne infrastrukture kot tudi na varnost ostale informacijske infrastrukture. Med najbolj odmevnimi ranljivostmi, ki so neposredno vplivale tudi na varnost komunikacijskih omrežij, so ranljivosti imenovane

Heartbleed, Poodle in Shellshock (Kinger, 2015). Heartbleed in Poodle sta ranljivosti v šifrirnih protokolih in knjižnicah, ki zagotavljajo šifriranje komunikacije med različnimi informacijskimi sistemi, uporabniki in napravami. Pri ranljivosti Poodle napadalec vpliva na postopek izbire šifrirnega algoritma med procesom vzpostavljanja šifrirane komunikacije s protokolom TLS/SSL. Protokol zaradi združljivosti s starejšimi sistemi omogoča uporabo različnih šifrirnih algoritmov. Napadalec z vplivanjem na podatkovni tok med odjemalcem in strežnikom doseže uporabo ranljivega oziroma manj varnega šifrirnega algoritma SSL 3.0, kar mu omogoči, da lahko z izrabo ranljivosti v šifrirnem algoritmu SSL 3.0 dešifrira komunikacijo med odjemalcem in strežnikom (Möller, Duong & Kotowicz, 2014). Pogoj za izvedbo tega napada je neposredni vpliv na tok podatkov, torej mora imeti napadalec bodisi fizični dostop do omrežja bodisi dostop do neke naprave v omrežju, ki mu omogoča prestrezanje in spreminjanje podatkovnega toka. Zaradi tega je napad na to ranljivost težje izvedljiv in posledično tudi manj verjeten (US-CERT, 2014). To pa ne velja za ranljivost Heartbleed. Heartbleed je ranljivost v odprtokodni šifrirni knjižnici OpenSSL, ki se uporablja v velikem številu varnostnih rešitev, od varnih dostopov, spletnih strani in elektronske pošte, do različnih izvedb navideznih zasebnih omrežij. Z izrabo napake v protokolu za vzdrževanje seje, lahko napadalec na daljavo in na enostaven način pridobi uporabniška imena in gesla trenutno aktivnih uporabnikov, v nekaterih primerih pa tudi zasebne ključe digitalnih potrdil, s katerimi je zaščitena komunikacija med odjemalcem in strežnikom. Ranljivost je bila v programski kodi prisotna od 14. marca 2012, inženirji podjetja Google pa so jo odkrili več kot dve leti kasneje. 21. marca 2014 so sami razvili popravek za ranljivost, o njej obvestili svoja partnerska podjetja, nekaj dni kasneje pa razvijalce šifrirne knjižnice in s tem tudi javnost. Uradni popravek s strani razvijalcev šifrirne knjižice OpenSSL je bil izdan šele 7. aprila 2014 (Codenomicon, b.l.; MITRE, b.l.; Roberts, 2014). Ranljivost je ogrožala veliko število sistemov po celem svetu in posledično tudi zasebnost velikega števila uporabnikov različnih internetnih storitev. Rezultati spletne ankete podjetja Netcraft kažejo, da je aprila 2014 kar 66 % svetovnih spletnih strežnikov uporabljalo programsko opremo, ki je za zagotavljanje šifriranja komunikacije uporabljala takrat še ranljivo knjižnico OpenSSL (Netcraft, 2014). Obseg razsežnosti ranljivih sistemov nam oriše informacija, da so bili ranljivi tudi sistemi podjetij Google, Cloudflare, Akamai in Facebook, njihove storitve pa uporabljajo milijoni zasebni uporabnikov in podjetij (Roberts, 2014). Poleg ranljivosti Poodle in Heartbleed pa veliko težav skrbnikom informacijskih sistemov, strežnikov in omrežji še vedno povzroča ranljivost v lupini Bash. Ranljivost, poimenovana Shellshock, je bila v mnogih različicah lupine prisotna kar 22 let, napadalcu pa omogoča oddaljeno izvedbo ukazov na ranljivem sistemu in posledično popolno kontrolo nad oddaljenim sistemom. Zaradi integracije lupine v jedro mnogih sistemov in naprav, je ranljivost možno izrabiti na različne načine, kot na primer preko protokola za samodejno dodeljevanje IP naslovov ob priklopu naprave v omrežje - DHCP ali protokola za prenos elektronske pošte - SMTP, ki sta široko uporabljana protokola v različnih komunikacijskih omrežjih po celem svetu (MITRE, b.l.). Razsežnost in vpliv vseh teh ranljivosti je, poleg široke uporabe, velik tudi zato, ker te šifrirne protokole različni standardi, vključno s standardom 27033, definirajo kot učinkovito sredstvo za varovanje komunikacijskih omrežij in sistemov (ISO, 2010, 2013b).

Zaščita omrežja pa ne pomeni samo zaščite aktivne omrežne opreme. V čim večji meri je treba zaščititi vse naprave, ki so priključene na omrežje. Kot je opisano že v točki 3.2.2, so omrežja največkrat le sredstva, ki napadalcem omogočajo oddaljen dostop do ranljivih sistemov in posledično podatkov, ki jih iščejo. Po večini standardi zahtevajo ščitenje omrežij na način, ki dovoljuje komunikacijo iz bolj varnih omrežij proti manj varnim. V obrani smeri mora biti posamezna komunikacija dovoljena le selektivno, prav tako pa se mora vsa prenesena vsebina v čim večji meri pregledati proti morebitnim napadom. Tak način varovanja ščiti naprave v notranjem omrežju organizacije pred neposrednim dostopom iz manj varnih omrežij, kot je na primer internet. Morebitni napadalec zato ne more neposredno napasti delovne postaje uporabnika, saj ta zanj ni neposredno dostopna. To pa žal zagotavlja varnost le pred osnovnimi tehnikami napadov, ne zagotavlja pa varnosti pri uporabi tehnik naprednih trajnih groženj, opisanih v točki 3.2.2. Napadalec lahko uporabi kombinacijo različnih tehnik napadov in socialnega inženiringa. Uporabniku lahko preko elektronske pošte pošlje posebej pripravljeno škodljivo kodo za izrabo ranljivosti v uporabniški programski opremi. Ko uporabnik priponko odpre, zažene škodljivo kodo, ki s strani uporabnikovega sistema do napadalčevega vzpostavi povratno kontrolno povezavo, preko katere napadalec dobi popoln dostop in nadzor nad uporabnikovim sistemom. Eno bolj odmevnih serij takšnih napadov v poročilu o napadu na bančne ustanove opisuje podjetje za informacijsko varnost Kaspersky. Po njihovih ocenah je skupina hekerjev med letoma 2013 in 2015 na tak način napadla sto svetovnih bank in jih oškodovala za milijardo dolarjev. Napadalci so izrabljali različne ranljivosti v programski opremi delovnih postaj uporabnikov bančnih storitev in bančnih uslužbencev. Z dostopom do delovnih postaj bančnih uslužbencev so pridobili posredni dostop do varovanih omrežij znotraj banke. V enem od primerov so z dostopom do postaje za nadzor bančnih avtomatov, z uporabo že nameščenih orodij za testiranje in nadzor bančnih avtomatov, ukradli kar 7,5 milijona dolarjev. Vse to je napadalcem uspevalo izvajati kar dve leti, kljub temu, da so banke sledile različnim varnostnim standardom in uporabljale različne varnostne rešitve, kot na primer šifriranje povezav in komunikacije, različne mehanizme prepoznavanja uporabnikov za dostop do sistemov, protivirusne programe ter sisteme za zaznavanje in preprečevanje vdorov (Kaspersky, 2015; Lennon, 2015). V tem primeru je bolj kot različne ranljivosti napadalcem dostope do delovnih postaj in drugih sistemov znotraj omrežja bank omogočila tehnika pridobivanja dostopa s povratno kontrolno povezavo, ki jo je možno z relativno enostavnimi varnostnimi mehanizmi zaznati in preprečiti (Gu, Zhang & Lee, 2008). Uspešna obramba pred naprednimi trajnimi grožnjami zahteva visok nivo tehnične in organizacijske varnosti, z velikim poudarkom na ozaveščanju ljudi. Primer zelo učinkovitega napada je napad na ameriško ministrstvo za zunanje zadeve konec leta 2014. Na ameriškem ministrstvu za zunanje zadeve so sredi novembra odkrili vdor v njihov sistem za neklasificirano elektronsko pošto (Chiacu & Brunnstrom, 2014). Izklop sistema za elektronsko pošto in povezave z javnim omrežjem, pregledovanje notranjih sistemov in delovnih postaj, iskanje orodij napadalcev in njihovo odstranjevanje, je bila dolgotrajna vojna med napadalci in varnostnimi inženirji različnih organizacij, ki so ministrstvu pomagale pri zajezitvi napada. Vsakokrat, ko so našli in odstranili nameščeno zlonamerno programsko opremo, so napadalci priredili izvorno kodo do te mere, da je varnostni sistemi niso zaznali in ponovno vdrli v njihov sistem (Yadron, 2015). Zajezitev

vdora in uspešno očiščenje sistemov jim je uspelo šele več kot štiri mesece po tem, ko so vdor zaznali in začeli s čiščenjem sistemov, pri čemer so morali večino sistemov na novo pripraviti in namestiti v omrežje (Hayes, 2015; Martosko, 2015). To nam kaže, da je varovanje pred naprednimi tehnikami napadov izredno težko, še težje pa je po uspešnem vdoru v informacijske sisteme te očistiti in jih ponovno pridobiti pod nadzor.

V nadaljevanju bom naredil analizo dostopnosti različnih orodij za izvajanje napadov, ki lahko varnostnim inženirjem pomagajo pri vzpostavljanju osnovne varnosti v njihovem omrežju.

3.4 Dostopnost orodij za izvajanje napadov

Internet ponuja dostop do velikega števila brezplačnih in komercialnih orodij za izvajanje različnih tipov napadov. Metodologija napada je po Andressu in Winterfeldu (2014, str. 24) proces treh korakov, in sicer poizvedovanje, napad in izraba ranljivosti. Za izvedbo vsakega posameznega procesa, napadalci uporabljajo več različnih orodij in tehnik, s katerimi zmanjšajo možnost, da bi jih odkrili.

V koraku poizvedovanja se uporabljajo različna orodja za pregledovanje omrežij in storitev, vohljanje za paketi in kreiranje IP paketov. Med najbolj znanimi orodji, ki se uporabljajo za pregledovanje omrežij in storitev, so Nmap, Nessus in Kismet. Nmap omogoča pregledovanje omrežij in storitev, določanje operacijskega sistema ciljnega sistema, različic programske opreme storitev na sistemu, zaznavanje ranljivosti, določanje tipa filtriranja paketov, določanje tipa požarnih pregrad in podobno (Lyon, b.l.). Nessus je eno bolj znanih in uporabljanih orodij, ki omogoča pregledovanje omrežij, preverjanje ranljivosti, presojo ustreznosti z različnimi standardi, presojo nastavitev ciljnih sistemov, itd. (Teenable Network Security, b.l.). Kismet je detektor brezžičnih omrežij, ki s pasivnim nadzorovanjem spektra brezžičnih omrežij uporabniku podaja različne informacije o brezžičnih omrežjih v njegovem dosegu (Kershaw, b.l.). Poleg orodij za pregledovanje omrežij napadalci uporabljajo tudi tako imenovana orodja za vohljanje za paketi. Ta orodja s pasivnim pregledovanjem podatkovnega toka uporabniku omogočajo vpogled v pakete na ožičenih in brezžičnih omrežjih, podajajo informacije o prenesenih podatkih, uporabljenih protokolih, tipu komunikacije itd. Najbolj uporabljana orodja so Wireshark, Ettercap, Tcpdump Aircrack-ng, v to kategorijo pa spada tudi del funkcionalnosti prej opisanega orodja Kismet (Andress & Winterfeld, 2014, str. 25). Wireshark, Ettercap in Tcpdump so orodja, ki omogočajo osnovno pregledovanje podatkovnega toka na vseh nivojih OSI referenčnega modela. Orodje Aircrack-ng omogoča vse naštete funkcionalnosti orodja Kismet, poleg tega pa tudi različne metode ugibanja in razbijanja zaščitnih ključev brezžične komunikacije. V fazi poizvedovanja pa največkrat niso dovolj le orodja za pasivno pregledovanje podatkovnih tokov in pregledovanje omrežij. Pri zaznavanju ciljnih sistemov in požarnih pregrad ter IDS/IPS sistemov na poti med napadalcem in njegovim ciljem, se uporabljajo tudi različna orodja, s katerimi lahko napadalec ročno naredi IP paket z vsemi različnimi možnostmi, ki jih protokol omogoča. V pakete lahko vključi različne anomalije, kar mu na podlagi odzivov sistemov omogoča odkrivanje različnih ranljivosti na končnih sistemih

ter morebitne sisteme na poti do ciljnega sistema, ki promet filtrirajo, normalizirajo in na druge načine pregledujejo. Dve najbolj znani orodji sta Netcat in Hping, katerih knjižnice so tudi del naprednejših orodij za izvajanje napadov (Andress & Winterfeld, 2014; Shakarian et al., 2013).

V koraku napada oziroma vdora v sisteme napadalci uporabljajo različna orodja za izrabo ranljivosti v aplikacijah in storitvah ter orodja, s katerimi na različne načine pridobivajo gesla uporabnikov, vse napade pa navadno tudi kombinirajo z raznimi tehnikami izogibanja zaznave napadov in socialnim inženiringom. Eno najbolj znanih in najbolj uporabljanih orodij oziroma ogrodij za izvajanje različnih vrst napadov je Metasploit. Metasploit vsebuje kopico različnih orodij in vtičnikov, ki omogočajo vse potrebno za fazo poizvedbe, fazo napada in fazo izrabljanja ranljivosti. Omogoča pregledovanje ciljnega sistema ter testiranje odprtih storitev za dovzetnost na posamezne napade na znane ranljivosti. Z vklopom modula za izrabo ranljivosti lahko napadalec izbere tip ranljivosti, ki jo želi izkoristiti za vdor na ciljni sistem, izbere akcijo, ki se na sistemu izvede po uspešnem vdoru, kot na primer namestitev programske kode za vzpostavitev kontrolne seje z napadenim sistemom in izbere tehniko za izogibanje zaznave napada oziroma vdora. Metasploit vsebuje tudi različne module za ustvarjanje napadov z ribarjenjem, ki jih lahko preko elektronske pošte ali z namestitvijo na neko spletno stran napadalec uporabi za pridobivanje dostopa do uporabnikovega sistema. Dobro podprti so tudi moduli za izvajanje napadov z vrinjenjem zlonamerne kode na spletne strani ter izvajanje raznovrstnih napadov na SQL strežnike. Zaradi široke uporabe se ob vsaki novo zaznani ranljivosti v programski opremi hitro pojavi modul ali vtičnik za izrabo te ranljivosti. Podobno orodje je tudi Canvas, ki sicer nima tako velikega nabora funkcionalnosti in modulov za izrabo ranljivosti, se pa za to orodje občasno na spletu pojavijo moduli za izrabo ranljivosti preden so znane javnosti (Andress & Winterfeld, 2014; McClure, Scambray & Kurtz, 2009; Weidman & Eeckhoutte, 2014).

Poleg posameznih ogrodij in programske opreme pa je na spletu možno dobiti tudi različne varnostne distribucije, ki vsebujejo operacijski sistem in skupek različnih orodij za varnostna testiranja, izrabljanje ranljivosti, računalniško forenziko itd. Ena najbolj znanih in široko uporabljanih varnostnih distribucij je Kali Linux. S skupkom različnih orodij se največkrat uporablja za penetracijska testiranja in računalniško forenziko, vključuje pa tudi vsa do sedaj našteta orodja in ogrodja (Andress & Winterfeld, 2014; McClure et al., 2009; Weidman & Eeckhoutte, 2014).

Poleg vseh naštetih aplikacij pa napadalci v veliko primerih uporabljajo tudi različna orodja za razbijanje gesel. Najbolj popularni orodji sta Cain and Able in John the Ripper, ki napadalcem omogočata napad na gesla s slovarji, grobo silo in dešifriranjem gesel pri uporabi reverznih algoritmov šifriranja (Andress & Winterfeld, 2014; Weidman & Eeckhoutte, 2014). Za pomoč pri pridobivanju dostopov, gesel in ostalih pomembnih podatkov pri izvajanju napadov napadalci največkrat uporabljajo tudi različna orodja za socialni inženiring, kot sta Social Engineering Toolkit in Maltego. Orodji omogočata iskanje ključnih besed po različnih forumih, socialnih straneh, podpornih straneh različnih proizvajalcev itd. Napadalec lahko z uporabo teh

orodij poišče, kaj je skrbnik varnostnih sistemov neke organizacije pisal ali spraševal na podpornih straneh in forumih proizvajalcev, kar mu omogoči vpogled v morebitne težave pri delovanju varnostnih sistemov. Orodji pokažeta tudi povezave z drugimi osebami na socialnih straneh, naslovni prostor, iz katerega se povezuje na različne spletne strani in podobno. Ta orodja se lahko uporabljajo v vseh fazah vdora, saj lahko preko njih napadalec tudi ugotovi, ali so v organizaciji izvedenemu vdoru mogoče na sledi.

Na spletu pa je mogoče najti tudi veliko število različnih orodij za izogibanje zaznave napada na IDS/IPS sistemih. Najbolj znani med njimi so Fragroute, Nikto, ADMutate, Havijis in Metasploit, za testiranje IDS/IPS sistemov in požarnih pregrad pa FTester, IDSprobe in Evader (Cheng et al., 2012, str. 3-5). Orodja omogočajo uporabno različnih znanih ranljivosti in težav pri zaznavanju anomalij ter napadov v IDS/IPS sistemih, napadov na SQL strežnike z vrinjenjem ukaznih nizov in podobno. Večina teh orodij je integriranih tudi v Metasploit ogrodje, kjer lahko različne tehnike kombiniramo v stilu naprednih trajnih groženj (Weidman & Eeckhoutte, 2014).

Število prosto dostopnih orodij in ogrodij, ki omogočajo napredne napade na informacijske sisteme in omrežja, je veliko. Večina jih je sicer namenjena varnostnim inženirjem za testiranje varnosti lastnega omrežja in storitev, jih je pa moč uporabiti tudi v zle namene. V nadaljevanju bom opisal sodobne tehnike in tehnologije varovanja komunikacijskih omrežij, ki naj bi omrežje in informacijsko infrastrukturo vsaj v večji meri obvarovale pred prej opisanimi napadi.

4 SODOBNE TEHNIKE IN TEHNOLOGIJE VAROVANJA KOMUNIKACIJSKIH OMREŽIJ

Varovanje komunikacijskih omrežij zahteva stalno spremljanje novih tipov napadov, novih tehnik in tehnologij varovanja, ranljivosti v sistemski in programski opremi ter njihovo redno odpravljanje, redno izvajanje varnostnih pregledov in penetracijskega testiranja ter tudi stalno ozaveščanje zaposlenih o socialnem inženiringu ter informiranje o raznih pasteh na spletnih straneh in v elektronski pošti.

4.1 Zaščita komunikacijskega omrežja

Zaščita komunikacijskega omrežja sega od povezovalnih kablov in brezžičnih omrežij pa do uporabnikov omrežja, torej posameznega človeka. Če želimo omrežje zaščititi pred vsemi nevarnostmi, moramo preprečiti pasivne in aktivne napade na omrežje in omrežne elemente, ne smemo pa pozabiti tudi na zaščito komunikacije pri uporabi mobilnih dostopov in zasebnih ali javnih storitev v oblaku.

4.1.1 Zaščita pred pasivnimi napadi

Vsako varovanje se začne na fizičnem nivoju in prav tako se na tem nivoju začne tudi varovanje omrežij. Fizični sloj povezave je lahko kabelski vod znotraj organizacije, MPLS omrežje ponudnika, najeta optična povezava med dvema zgradbama ali kakršni koli tip brezžičnega omrežja. Fizičnega varovanja kabelskih povezav znotraj organizacije v večini primerov ni težko zagotoviti. Težje pa je to pri najetih povezavah med različnimi oddaljenimi poslovnimi enotami organizacije in pri uporabi različnih brezžičnih omrežij, kot na primer povezave med poslovnimi stavbami, lokalno brezžično omrežje znotraj poslovne stavbe, osebna brezžična omrežja in podobno. Varnost v vseh naštetih omrežjih je možno zagotoviti s šifriranjem komunikacije oziroma komunikacijskega kanala na prvem, drugem, tretjem in sedmem nivoju OSI modela. Šifriranje na prvem nivoju OSI modela nam omogočajo optični multiplekserji, ki zagotavljajo šifriranje in izmenjavo šifrirnih ključev z različnimi kvantnimi metodami (Akhgar & Arabnia, 2013; Kartalopoulos, 2008). Druge oblike šifriranja se izvajajo na višjih nivojih. Tako brezžični usmerjevalniki kot različna omrežna stikala omogočajo šifriranje na drugem sloju OSI modela. Za brezžična omrežja je takšno šifriranje dandanes njuno, pri ožičenih omrežjih pa se uporablja predvsem tam, kjer infrastruktura objekta dovoljuje neavtoriziran dostop do omrežnih kablov. Šifriranje na višjih nivojih je učinkovito za povezave med različnimi končnimi točkami v omrežju, ki so lahko naprave uporabnikov, omrežne naprave, samostojne naprave itd. Najbolj uporabljani šifrirni protokoli so IPSEC, PPTP/L2TP, ki delujeta na tretjem nivoju, ter SSH in TLS/SSL na sedmem nivoju (Akhgar & Arabnia, 2013; Andress, 2014; Daya, 2013; Kartalopoulos, 2008). S šifriranjem morebitnemu napadalcu preprečimo dostop do podatkov na komunikacijski poti, vendar se je pri tem treba zavedati, da je varnost šifrirane komunikacije odvisna le od zmožnost napadalca, da odkrije tip šifriranja in pridobi šifrirne ključe ali dobi dostop do podatkov, preden se začnejo šifrirati. Zato je treba poskrbeti tudi za varnost naprav, ki šifriranje izvajajo, ter morebitnih delovnih postaj, ki imajo dostop do teh naprav. Preko teh bi napadalec lahko prišel do podatkov o šifrirnih algoritmih ter pridobil ključe, s katerimi je komunikacija šifrirana (Kartalopoulos, 2008, str. 1).

4.1.2 Zaščita pred aktivnimi napadi

Če želimo omrežje zaščititi pred aktivnimi napadi, moramo ščititi vso aktivno omrežno opremo kot tudi vse ostale naprave, ki so priključene na omrežje. Napadalec lahko tudi z vdorom v različne uporabniške naprave, kot so na primer tiskalniki, delovne postaje, brezžične dostopne točke, brezžična terminalna oprema itd., pridobi dostop do notranjih omrežnih elementov.

Zaščito omrežja sestavljajo usmerjevalniki in stikala z nameščenimi seznami za nadzor dostopa, večnamenske požarne pregrade, IDS/IPS sistemi, posredniški strežniki, sistemi za odkrivanje botnet komunikacije, naprave za filtriranje dostopov do spletnih naslovov in aplikacij, sistemi za zaznavanje naprednih trajnih groženj, navidezna zasebna omrežja, šifriranje in dešifriranje prometa ter segmentacija omrežij (Akhgar & Arabnia, 2013; Daya, 2013; ISO, 2009, 2010, 2012, 2013c, 2014; McClure et al., 2009). Večino naprav in tehnologij sem opisal že v prejšnjih

poglavjih, zato se bom v tem poglavju osredotočil na novejšo tehnologijo in zaščito pred napadi in vdori.

Kljub temu, da novejših napadov klasične tehnike in tehnologija uporabe seznamov za nadzor dostopa, požarnih pregrad in IDS/IPS sistemov največkrat ne ustavijo, so te še vedno pomembne za celovito zagotavljanje varnostni. Nove tehnike izogibanja zaznave napadov pa zahtevajo novejše pristope. Novejše požarne pregrade morajo delovati na več nivojih hkrati in večinoma vsebujejo tudi module z IDS/IPS sistemi, module za protivirusno pregledovanje prometa, dešifriranje SSL sej, nadzor dostopa do spletnih strani in aplikacij, modul za posredniški strežnik, modul za preprečevanje uhajanja podatkov, sisteme za odkrivanje botnet komunikacije in vmesnike za priklop sistemov za zaznavanje naprednih trajnih groženj. Klasične požarne pregrade počasi zamenjujejo požarne pregrade nove generacije in naprave za celovito upravljanje s tveganji (v nadaljevanju UTM naprava). Prednost teh naprav je, da posamezni moduli v večji meri delujejo integrirano in omogočajo naprednejše tehnike preverjanja posredovanega podatkovnega toka. Prvo filtriranje prometa izvede modul požarne pregrade, ki ima pri požarnih pregradah novejšega tipa tudi možnost prepoznavanja uporabnikov končnega sistema in tako omogoča pisanje pravil ter filtriranje komunikacije glede na uporabnika in ne le glede izvornega IP naslova. Navadno UTM naprave že na tej stopnji omogočajo tudi dešifriranje šifrirnih protokolov, kot je na primer SSL, kar modulom omogoča vpogled v podatkovni tok, ki je pri prenosu preko omrežij šifriran. Omejitve takšnega pregledovanja sem opisal že v točki 1.2, zato jih tu ne bom ponavljal. Po končanem filtriranju UTM sistem prejeti promet razpošlje ostalim modulom. Navadno požarni pregradi sledijo IDS/IPS moduli, ki s podpisi znanih napadov ter preverjanjem anomalij zaznavajo in preprečujejo napade na omrežja. Novejši IDS/IPS sistemi pregledujejo pakete na vseh nivojih z uporabo tako imenovane normalizacije, kar omogoča naprednejšo zaznavo različnih tehnik izogibanja zaznavi. Naslednja stopnja so navadno moduli za filtriranje dostopov do spletnih strani in spletnih aplikacij. Ti moduli s preverjanjem klasifikacije ciljne spletne strani glede na nastavljeno politiko uporabniku dostop dovolijo ali preprečijo. Ponudniki klasifikacijskih baz tudi redno pregledujejo spletne strani za vsebnost virusov in škodljive programske opreme, kar pomaga organizaciji pri preprečevanju napadov z ribarjenjem in nezavedno okužbo delovnih postaj uporabnikov. V tej fazi UTM sistem promet pregleduje tudi za vsebnost botnet komunikacije. Različni proizvajalci UTM sistemov za zaznavanje botnet komunikacije ponujajo različne rešitve, največ pa jih temelji na iskanju znanih botnet ukazov z uporabo podpisov in pregledovanjem DNS zahtev. Slednje izvajajo na dva načina, in sicer z iskanjem domenskih imen v bazi znanih botnet domen in na podlagi naključno ustvarjenih domenskih prefiksov, ki so znani za botnet omrežja (Gu et al., 2008, str. 5-9). Ves promet UTM sistem pregleduje tudi za vsebnost virusov in uhajanje zaupnih podatkov. Modul za preprečevanje uhajanja zaupnih podatkov vsebuje podpise in različne definicije klasificiranih podatkov, ki mu omogočajo zaznavanje različnih podatkov zaupne narave v dokumentih in besedilu. V primeru zaznave prenosa zaupnega dokumenta ali besedila lahko komunikacijsko sejo prekine in o tem obvesti odgovorne osebe. Po pregledu paketa ali podatkovnega toka, je ta posredovan proti cilju komunikacije, nekateri UTM sistemi pa omogočajo tudi posredovanje prometa na sisteme za

zaznavanje naprednih trajnih groženj, ki so trenutno najbolj napredna tehnologija v boju z naprednimi trajnimi grožnjami. Večinoma so to samostojne naprave, ki jih lahko priklopimo na poseben vmesnik UTM sistema ali pa pasivno na omrežje z uporabo sistema za zrcaljenje povezave. Naprave z analizo prejetega prometa iz njega izluščijo vse prenesene datoteke, spletne strani, vtičnike itd. ter jih posredujejo različnim navideznim delovnim postajam, ki simulirajo obnašanje uporabnika. To pomeni, da z uporabo različnih programov in skript na različne načine zaganjajo prejete datoteke, ob tem pa natančno nadzorujejo delovanje gostiteljskega sistema, porabo virov, omrežni promet iz gostiteljskega sistema proti ostalemu omrežju itd. Če pri tem zaznajo anomalijo v delovanju sistema, sprožijo alarm in s tem odgovorne osebe opozorijo na sumljivo aktivnost na omrežju. Na ta način je moč zaznati veliko število napadov, ki jih varnostni sistemi, ki temeljijo na podpisih napadov, ne morejo zaznati. Imajo pa UTM sistemi dve pomanjkljivosti. Prva pomanjkljivost je čas, ki ga potrebujejo za pregled prometa. Simulacija lahko traja tudi do nekaj minut, zaradi česar tovrstni sistemi ne morejo biti aktivno umeščeni v omrežje in sproti preprečevati napadov. Alarm, ki ga ustvarijo, je v mnogih primerih tako že prepozen, saj je v času simulacije promet prispel tudi do uporabnikove naprave, kjer obstaja velika možnost, da se je škodljiva programska koda že zagnala. Dobra stran pri tem je, da so odgovorne osebe o tem hitro obveščene in lahko s hitro reakcijo okužbo omejijo. Druga slaba stran UTM sistemov pa je uporaba navideznih okolij za izvajanje simulacij. Novejša škodljiva programska oprema namreč že omogoča zaznavanje izvajanja v navideznem okolju, prav tako pa zna zaznati, ali neke ukaze in akcije na sistemu izvaja človek ali skripte (Andress & Winterfeld, 2014; Daya, 2013; ISACA, 2014; McAfee, 2015; Niemi, 2013).

4.2 Odpravljanje ranljivosti

Odpravljanje ranljivosti oziroma nameščanje varnostnih popravkov je eden bolj kritičnih procesov za zagotavljanje informacijske varnosti. Z vedno večjim poudarkom na varnih omrežjih in sistemih je tudi večina proizvajalcev programske in strojne spremenila in pohitrila postopke odprave ranljivosti. V letu 2014 je kar 83,1 % proizvajalcev ponudilo popravke za ranljivosti v lastni opremi na dan razkritja ranljivosti. Leta 2009 se je ta vrednost gibala okoli 50 %, odprava napake v 30 dneh po razkritju pa le okoli 55 % (Secunia, 2015, str. 11). Kljub hitremu dostopu do popravkov, pa skrbniki raznih sistemov te popravke veliko počasneje nameščajo. Če pogledamo najbolj znano ranljivost v letu 2014 z imenom Heartbleed, je po podatkih SI-CERT (2015, str. 19) v prvem mesecu po razkritju ranljivosti v Sloveniji popravke na sisteme namestilo le okoli 50 % skrbnikov, tri mesece po razkritju pa je brez popravkov ostalo še okoli 37 % sistemov. Zanimivo pri tem je, da je večina proizvajalcev IDS/IPS sistemov ponujalo podpise za zaznavanje Heartbleed napada že na dan razkritja, kar pomeni, da teh 50 oziroma 37 % sistemov bodisi ni zaščiteno z IPS sistemi bodisi pa tudi na njih ves ta čas niso bili nameščeni in aktivirani podpisi novih omrežnih napadov.

Nameščanje popravkov v velikih sistemih je lahko zelo dolgotrajen postopek, predvsem v sistemih, ki morajo delovati neprestano. Če organizacija nima vzpostavljene testne

infrastrukture, kjer lahko popravke hitro namesti in preveri funkcionalnost njihovih storitev z nameščenimi popravki, lahko proces nameščanja popravkov neposredno na produkcijske sisteme pripelje do različnih nevšečnosti, kot na primer spremembo delovanja posameznih sistemov ali odpovedi določenih funkcionalnosti sistema. Še bolj pa je to kritično na omrežni opremi. Omrežno opremo je treba največkrat nadgrajevati izven delovnega časa organizacije oziroma med urami z najmanjšo izpostavljenostjo uporabnikov izpadu sistema. Ker se lahko zaradi testiranja in načrtovanja nameščanja popravkov ali novejših različic operacijskih sistemov na aktivne omrežne naprave to zavleče tudi za več tednov ali mesecev, je v vmesnem času nujno zagotoviti zmanjšanje tveganja na druge načine. Pri tem so nam lahko v veliko pomoč IPS sistemi, za katere lahko po potrebi tudi sami razvijemo podpise za zaznavanje nekega, za nas kritičnega napada. Organizacija mora poleg dobro razvitih postopkov za nameščanje popravkov, razviti postopke zagotavljanja varnosti ob razkritju ranljivosti. Pri tem pa ni pomemben le čas po razkritju ranljivosti. Ranljivosti Heartbleed in Shellshock sta bili v različnih sistemih prisotnih več let, slednja kar 22 let. Seveda je najbolj kritičen čas med uro razkritja ranljivosti in namestitvijo popravkov na ranljive sisteme ali podpisov na IPS naprave organizacije, veliko težo pa nosi tudi čas med prvo izdajo ranljive programske opreme in razkritjem ranljivosti (Codenomicon, b.l.; McAfee, 2015; Reiske, 2014). Organizacije bi morale vzpostaviti sistem hranjenja posnetka prometa med različno varnimi omrežji za neki določen čas na način, ki bi organizaciji omogočal ob razkritju ranljivosti ugotavljanje ali je bilo omrežje organizacije z novo razkrito ranljivostjo v preteklosti že napadeno.

4.3 Varnostni pregledi in njihova uporabnost

Različni standardi, vključno s standardom ISO/IEC 27033, priporočajo izvajanje letnih varnostnih pregledov. Cilj varnostnega pregleda je ocena odstopanja varnostne arhitekture in njenega stanja od zahtev standardov in varnostne politike, mnogokrat pa sta kot del varnostnega pregleda narejena tudi ocena ranljivosti in penetracijsko testiranje posameznih sistemov ali celotne informacijske infrastrukture. Končno poročilo dobro izvedenega varnostnega pregleda je za varnost sistemov v organizaciji ključnega pomena, predvsem v primerih, ko izvajalci zaznajo kritične nepravilnosti in pomanjkljivosti v varnostni politiki, njenemu izvajanju ali varnostni arhitekturi omrežja. Pri tem pa je zelo pomembna ocena ranljivosti. Pri oceni ranljivosti izvajalci preverijo, ali v operacijskih sistemih, aplikacijah in storitvah obstaja kakšna znana ranljivost, ki je lahko posledica napačnih nastavitev, pomanjkljivega nameščanja varnostnih popravkov ali uporabe stare različice sistema oziroma aplikacije. Za izvajanje ocene ranljivosti izvajalci navadno uporabljajo različna varnostna orodja, ki so v večini opisana v točki 3.4. Ocena ranljivosti nam poda predvsem informacijo o splošni ranljivosti nekega sistema ali omrežja organizacije na znane pomanjkljivosti in ranljivosti v posameznih operacijskih sistemih in aplikacijah na dan izvedbe testiranja. Pri tem se je treba zavedati, da je, kljub teoretični 100 % zanesljivosti poročila, to lahko že naslednji dan, s pojavom novih ranljivosti in z njimi povezanih groženj, zastarelo. Organizacije morajo zato stalno slediti varnostnim priporočilom in opozorilom proizvajalcev programske in stojne opreme, ki jo uporabljajo. Enako je pri izvajanju penetracijskega testiranja, pri katerem poskušajo izvajalci z

izrabo različnih pomanjkljivosti in ranljivosti pridobiti dostop do čim večjega števila oziroma čim bolj zaščitenih sistemov organizacije. Tako kot poročilo ocene ranljivosti, je tudi poročilo penetracijskega testiranja aktualno le do naslednjega odkritja pomanjkljivosti ali ranljivosti, merodajnost obeh poročil pa je seveda odvisna od kakovosti izvedbe.

Varnostni pregledi so torej zelo uporabni predvsem pri razkritju pomanjkljivosti v varnostni arhitekturi in izvajanju določil standardov ter varnostne politike. Njihova uporabnost je zelo odvisna od kakovosti izvedbe, vrednost pa imajo le v zgodovinskem smislu, saj so lahko, zaradi hitrega spreminjanja tipov in tehnik napadov ter dnevnim pojavljanjem novih ranljivosti, informacijski in komunikacijski sistemi organizacije naslednji dan spet ranljivi.

V nadaljevanju bom pregledal razkorak med zahtevami standarda ISO/IEC 27033 in v predhodnih poglavjih opisanimi tipi in tehnikami sodobnih napadov na omrežja in opisanimi tehnikami in tehnologijami varovanja komunikacijskih omrežij.

5 PREGLED RAZKORAKA MED ZAHTEVAMI STANDARDA ISO/IEC 27033 IN SODOBNIMI TEHNIKAMI NAPADOV TER VAROVANJA KOMUNIKACIJSKIH OMREŽIJ

V tem poglavju bom analiziral razkorak med priporočili in zahtevami standarda ISO/IEC 27033 ter v tretjem in četrtem poglavju opisanimi tipi in tehnikami napadov na omrežja ter tehnikami in tehnologijami varovanja pred napadi.

5.1 Tehnike napadov na komunikacijska omrežja, pred katerimi standard ne opredeljuje učinkovitih priporočil in zahtev za zaščito

Posamezni deli standarda so bili izdani preko več let, zaradi česar se celotni standard dobro dopolnjuje. Prva dva dela, ki obravnavata teorijo varovanja, dobro pokrivata tematiko teoretičnega varovanja omrežij pred klasičnimi načini napadov. Občasno se sicer sklicujeta na tehnologijo, ki je v današnjih časih ni več priporočljivo uporabljati, a zadnji trije deli standarda, ki so bolj tehnično naravnani, te pomanjkljivosti po večini odpravijo. Priporočila in zahteve celega standarda dobro odpravljajo osnovne tehnike napadov, za varovanje pred naprednimi trajnimi grožnjami pa bi bilo treba standard razširiti.

Napredne trajne grožnje temeljijo na izrabljanju različnih vektorjev napadov in hitremu prilagajanju zlonamerne programske kode zmogljivostim zaznavanja. Največkrat je cilj napadov dolgoročno pritajeno pridobivanje podatkov ter informacij. Vdore v informacijske sisteme je težko preprečiti, ker uporabljajo najnovejše tipe ranljivosti, ki navadno javnosti še niso razkrite oziroma so razkrite zelo malo časa. Požarne pregrade, IDS/IPS sistemi, preverjanje vsebine komunikacije, protivirusni programi in podobni pristopi z uporabo podpisov znanih napadov so zato v fazi začetnega vdora neučinkoviti. Ker je začetni vektor napada največkrat

socialni inženiring, lahko organizacije za varnost svojega omrežja poskrbijo le z ozaveščanjem zaposlenih, kar standard tudi večkrat poudari. Poleg ozaveščanja pa mora organizacija vzpostaviti še učinkovit način odkrivanja že izvedenih vdorov. Cole (2013, str. 19) pravi, da so največkrat napadalci v omrežjih in na sistemih organizacije prisotni od šest do devet mesecev, preden organizacije vdore zaznajo. Učinkovitost novodobnih napadalcev je povezana z dolgotrajnim zbiranjem različnih informacij o organizaciji, njenih informacijskih in varnostnih sistemih ter njenih zaposlenih. Na podlagi zbranih informacij se nato odločijo za vektor napada, točko napada, v fazi napada pa največkrat uporabijo unikatno zlonamerno kodo, ki v večini primerov temelji na izrabi še neznanih ranljivosti. Da bi se organizacija lahko vsaj malo zaščitila pred naprednimi trajnimi grožnjami, mora zelo dobro poznati samo sebe ter razviti podoben način razmišljanja kot napadalci. Prvi korak je identifikacija sredstev organizacije, ki bi bila najverjetnejši cilj napadalca, torej najbolj kritične informacije organizacije. Na podlagi tega mora oceniti najbolj verjeten vektor napada, točko vdora, način izvedbe napada in tudi način zagotavljanja stalnega dostopa do informacijskih sistemov organizacije. Cole (2013, str. 22) ocenjuje, da je pri tovrstnih napadih točka vhoda največkrat uporabnik ali skupina uporabnikov, pri tem pa opozarja, da klasični načini odkrivanja napadov z uporabo podpisov znanih napadov niso učinkoviti, saj napadalci pri napadih izrabljajo še neznane ranljivosti, te pa kombinirajo z različnimi načini izogibanja zaznavi. Največkrat za izvedbo napada, predvsem pa za zagotavljanje stalnega dostopa do omrežja organizacije, uporabljajo različne načine normalizacije prometa. To pomeni, da so paketi napada zelo podobni ali enaki legitimnim paketom na omrežju, kar zopet oteži zaznavanje z različnimi varnostnimi sistemi. Ker je navadno želja napadalcev okužba čim več različnih sistemov, največkrat uporabljajo avtomatiziran napad. Ker je veliko sistemov hkrati težko očistiti zlonamerne kode, jim izraba večjega števila sistemov zagotavljala dolgoročnejši dostop do omrežja organizacije.

Kontrole, ki ji predvideva standard, so dobro oblikovane in zelo pomembne za varovanje omrežja pred različnimi klasičnimi tipi in tehnikami napadov, žal pa pred prej opisanimi napadi organizacije omrežij ne morejo zaščititi. Ti namreč zahtevajo drugačen pristop k varovanju omrežij. Standardu manjkajo predvsem principi zaznavanja in reševanja že izvedenih in uspelih vdorov v omrežja organizacije. V naslednjem poglavju bom opisal pristop k varovanju omrežij pred naprednimi trajnimi grožnjami in splošne pomanjkljivosti standarda.

5.2 Pomanjkljivosti standarda

Največja pomanjkljivost standarda je pomanjkljiv pristop k zagotavljanju varovanja omrežja pred novodobnimi napadi. Posamezne nadzorne točke so sicer dobro zastavljene, vendar je za novodobne napade potreben drugačen pristop k informacijski varnosti in posledično nadzornim točkam za njeno zagotavljanje. Poleg tega, da organizacija vzpostavlja in izvaja različne procedure upravljanja z ranljivostmi, skrbi za redno nadgrajevanja podpisov na IDS/IPS sistemih, protivirusnih sistemih ter sistemih za zaznavanje škodljive kode in ozavešča uporabnike, mora tudi zelo dobro razumeti samo sebe in novodobne napade ter vzpostaviti procedure za napredno zaznavanje že izvedenih vdorov in čiščenje zlorabljenih sistemov.

Dosedanji sistem občasnega pregledovanja sistemov in varovanja z nameščanjem popravkov in podpisov je treba nadgraditi s stalnim varovanjem omrežja, ki zahteva neprekinjeno sledenje novim ranljivostim, neprekinjeno revidiranje nameščenih aplikacij in storitev, zaznavanje anomalij v podatkovnih tokovih znotraj in zunaj omrežja organizacije ter sledenje novih tehnik in tehnologij vdiranja v informacijske in komunikacijske sisteme. Cole (2013, str. 23) za ustrezno zaščito pred naprednimi trajnimi grožnjami predlaga nadzor uporabnikov ter stalno ozaveščanje, pravilno rangiranje virov, dogodkov in uporabnikov, temeljito sledenje in pregledovanje prometa iz omrežja organizacije proti drugim omrežjem, poglobljeno razumevanje napadov ter zagotavljanje varnosti končnih točk v omrežju.

a) Izobraževanje in ozaveščanje

Izobraževanje in ozaveščanje uporabnikov standard večkrat omenja, več poudarka pa bi moralo biti na ustreznem ozaveščanju uporabnikov takoj ob pojavu novih možnosti vdorov. Tehnične zmožnosti preprečevanja novejših tipov in tehnik napadov so pri naprednih trajnih grožnjah dokaj neučinkovite, zato je samoomejevanje dostopov s strani uporabnika tukaj ključnega pomena. Uporabnik mora znati oceniti verjetnost napada tudi ob prejemu neke navidezno legitimne vsebine s strani poznane osebe.

b) Rangiranje virov, dogodkov in uporabnikov

Standard v fazi vzpostavljanja informacijske varnosti zahteva, da organizacija klasificira vire glede na predvidena varnostna tveganja. Da je lahko varnost omrežij učinkovita, pa bi morala organizacija vire, tveganja in dogodke rangirati glede na njihovo vedenje v trenutku njihove spremembe. Razlog je predvsem izredno težko zaznavanje naprednih trajnih groženj s starimi varnostnimi mehanizmi, saj maskirajo svojo komunikacijo z normalizacijo prometa. Organizacija mora zato nadzorovati dogodke in promet, ki ga ustvarjajo uporabniki in končni sistemi na omrežju, oceniti anomalije, jih na podlagi tega rangirati v skupine in določiti vzroke anomalij (Cole, 2013; Niemi, 2013).

c) Pregledovanje izhodnega prometa

Standard večinoma predlaga nadzorovanje prometa s strani manj varnega omrežja proti bolj varnemu omrežju. Le v enem primeru predlaga nadzorovanje prometa v obeh smereh, kar mora biti pri naprednih trajnih grožnjah minimalna zahteva vsake medomrežne povezave. Ker napadalci uporabljajo različne tehnike normalizacije prometa, in ker je njihov cilj večinoma dostop do podatkov in informacij, je treba povsod pregledovati promet na poti iz omrežja organizacije proti zunanjim omrežjem. S tem bo organizacija preprečila odtekanje podatkov in informacij v primeru uspešnega vdora v njene sisteme. Ker tudi pri odtekanju podatkov napadalci uporabljajo različne tehnike izogibanja zaznave, mora organizacija vzpostaviti dobro tehnično omejevanje dovoljenega prometa proti zunanjim omrežjem, pregledovanje prometa za vsebnost povratnih kanalov ter vzpostaviti tudi sisteme za preprečevanje odtekanja podatkov in

informacij. Pregledovanje mora biti v čim večji meri avtomatizirano, saj je množici napadov in anomalij nemogoče slediti ročno (Cole, 2013; ISACA, 2014).

d) Poglobljeno razumevanje napadov

Kritičnega pomena je tudi poglobljeno razumevanje novih tipov napadov. Tu bi moral standard priporočati oziroma zahtevati stalno seznanjanje varnostnega osebja z novimi tipi napadov, njihovimi prednostmi in slabostmi. Le tako bodo lahko predvideli točke ranljivosti lastnega omrežja in pripravili kontrole, ki bodo ranljivosti odpravile ali pa vsaj zagotovile hitro zaznavo njihove izrabe. Organizacija bi morala tudi vzpostaviti sistem, ki bi s sledenjem različic uporabljanih sistemov in aplikacij znotraj omrežja organizacije stalno primerjal z novo najdenimi ranljivostmi. To bi varnostnemu osebju omogočilo hitro odpravljanje ranljivosti in lažje zaznavanje izrabe (Cole, 2013; Niemi, 2013).

e) Varnost končnih točk

Varnost končnih točk je v standardu večkrat poudarjena, za zagotavljanje varnosti pa so specificirane tudi vse potrebne kontrole. Poudariti pa je treba, da je varnost končnih točk v veliki večini odvisna od njihovih uporabnikov, zato jih je treba stalno informirati, izobraževati in ozaveščati.

Poleg naštetih točk so ključni tudi postopki ob zaznavi vdora. Standard bi moral predpisati postopke za varovanje omrežja v času med objavo ranljivosti in objavo popravkov za ranljivost oziroma podpisov za IDS/IPS sisteme. To bi bilo lahko na primer pisanje lastnih podpisov za zaznavanje napada ali morebiti tudi izolacija storitve oziroma sistema za čas do odprave ranljivosti. Standard bi moral tudi opredeliti oziroma predlagati sistematični pristop k odpravi vdora v različne sisteme organizacije. Procedure bi morale vključevati principe reševanja vdorov, postopke odpravljanja ranljivosti in čiščenja zlonamerne kode, postopke obveščanja drugih organizacij in organov pregona ter morebitno vzpostavitev ločenega nadomestnega sistema. Ta bi se uporabil v primeru, ko bi morala organizacija zaradi zagotavljanja minimalne stopnje varnosti podatkov in informacij primarno infrastrukturo ugasniti, nadomestni sistem pa bi v tem času zagotovil »čisto« kritično infrastrukturo. Postopki obnove sistema bi morali določati tudi načine čiščenja okuženih sistemov, kot na primer nova postavitev sistema v ločenem okolju, prirejanje novega sistema na odpornost pred zaznano zlonamerno kodo in zamenjava okuženega sistema z novim. Še ena kritična pomanjkljivost standarda so tudi predpisani načini varovanja omrežij pred napadi. Varovanje izključno meje med omrežji in končnih naprav je star koncept. Organizacija bi morala znotraj svojih omrežij uporabljati pasivno nameščene IDS sisteme, ki bi omogočali pregledovanje prometa in zaznavanje anomalij znotraj enega omrežja, ne samo med prehodom v druga omrežja. Ker napredne trajne grožnje večinoma temeljijo na izrabi ranljivosti ničelnega dne, bi bilo za organizacijo priporočljivo, da bi za določen čas hranila posnetek vhodnega in izhodnega prometa med omrežji organizacije z ostalimi omrežji. To bi organizaciji omogočilo, da bi po razkritju nove

ranljivosti in po prejemu IDS/IPS podpisov za njeno zaznavanje, posnetek prometa uporabila za preverjanje ali je bila morebiti v preteklosti ta ranljivost na sistemih organizacije že izrabljena (Cole, 2013; Del Carlo, 2003; Niemi, 2013).

Standard pa ima tudi nekaj pomanjkljivosti pri predlaganih varnostnih kontrolah, ki bi morale biti danes že stalnica varovanja omrežij. Na nivoju povezave omrežja organizacije z internetom bi moral standard predlagati tudi izvajanje filtriranja prometa glede na geografsko lokacijo njegovega izvora. S tem lahko neko podjetje v Sloveniji, ki posluje na primer le znotraj Evrope, do večine svojih storitev blokira dostope iz omrežij izven Evrope. S tem onemogoči napade na svoje omrežje iz držav, ki se največkrat pojavijo kot izvori napadov. Kot drugo zelo pomembno varnostno kontrolo bi lahko izpostavil zaščito DNS strežnikov in DNS razreševanja z uporabo DNSSEC protokola. Izraba različnih ranljivosti in pomanjkljivosti v nastavitvah DNS strežnikov in samega DNS protokola je skoraj stalnica pri različnih napadih na posamezne organizacije, države in celo večje regije. Enako bi moral standard zahtevati tudi zaščito dinamičnega usmerjanja znotraj omrežja organizacije in pri morebitni uporabi BGP protokola za povezovanje organizacije z internetom. To lahko prepreči zlonamerno preusmerjanje prometa organizacije preko omrežij ali omrežne opreme napadalcev, ki želijo promet pasivno prestrezati, aktivno vanj posegati ali pa s preusmerjanjem izvesti napad onemogočanja storitve. Standard pri preprečevanju slednjega tudi ne omenja potrebe vzpostavitve procedur s ponudniki dostopa do interneta za preprečevanje distribuiranega onemogočanja storitve v primerih, ko želijo napadalci s popolno izrabo pasovne širine preprečiti dostop organizacije do interneta in njenih strank do njenih storitev. Ker se je pred tovrstnim napadom nemogoče obraniti na strani omrežne opreme organizacije, mora imeti ta s ponudniki dostopa vzpostavljen postopek blokade porazdeljenih napadov onemogočanja storitve. Standard pri dostopu do interneta tudi nikjer ne predvideva uporabe IPv6 protokola, ki bi spremenil ali razširil mnogo predvidenih kontrol.

Na nivoju zagotavljanja varnosti notranjih omrežij organizacije bi moral standard v sklopu fizičnega varovanja dostopov do omrežja predlagati tudi uporabo algoritmov za overjanje omrežnih elementov, kot na primer 802.1x, ter uporabe šifriranja povezave med posameznimi omrežnimi elementi, kot na primer protokola Media Access Control Security. Pohiteti bi morali tudi z izdajo šestega dela standarda, ki obravnava varovanje vsak dan bolj uporabljanih brezžičnih omrežij ter predvideti še kontrole in smernice za varovanje povezav z omrežji in storitvami v oblaku ter varovanje in upravljanje programsko definiranih omrežij. Na nivoju upravljanja dostopov do omrežne opreme bi moral standard priporočati uporabo sistemov za upravljanje privilegiranih računov. Te sistemi omogočajo zakrivanje poverilnic privilegiranih računov na omrežni opremi in delujejo podobno kot posredniški strežniki. Skrbniki se z uporabo lastnih poverilnic povežejo na sistem, ki jih overi in jim glede na politiko dostopov dovoli dostope do specifičnih omrežnih sistemov. Sistem se nato s privilegiranim računom poveže na ciljni sistem ter med njim in skrbnikom posreduje ukaze, hkrati pa sejo skrbnika tudi posname za namene revizije. Nekateri sistemi omogočajo tudi avtoriziranje posameznih ukazov, ki jih želi skrbnik izvesti na končnem sistemu (Brewster, 2014; Younus, 2005).

SKLEP

Standard ISO 27033 v večji meri dobro pokriva teorijo in prakso varovanja komunikacijskih omrežij pred klasičnimi tipi napadov, med katere spadajo tudi napadi z različnimi avtomatiziranimi orodji. Nekajkrat sicer posamezni del standarda predlaga uporabo varnostnih protokolov, za katere danes menimo, da niso varni, a drugi deli standarda v večini primerov te pomanjkljivosti odpravijo. Velika pomanjkljivost standarda pa je vezana na zagotavljanje varnosti pred novodobnimi tipi napadov oziroma naprednimi trajnimi grožnjami. Tovrstni napadi so v veliki meri prilagojeni posamezni organizaciji, kar pomeni, da jih je zelo težko izslediti s klasičnimi varnostnimi kontrolami. Varovanje pred takšnimi napadi zahteva drugačno filozofijo, kot jo predstavlja standard. Ker je začetne vdore v omrežje organizacije težko odkriti, mora varnost temeljiti na iskanju anomalij v prometu in delovanju sistemov, iskanju zlonamerne kode in komunikacije znotraj omrežij ter natančnem preverjanju komunikacije, usmerjene iz omrežja organizacije proti zunanjim omrežjem. Ker to pomeni, da bo večina vdorov odkritih šele po uspešno izvedenem vdoru, bi moral standard predvideti tudi priporočila za odstranjevanje posledic vdora. Najbolj pomemben člen v zagotavljanju varnosti informacijskih in komunikacijskih sistemov pa je še vedno človek, kar standard tudi večkrat poudari. Ključno pomanjkljivost standarda pri zagotavljanju varnosti predstavljajo tudi manjkajoči zadnji del standarda, ki bi obravnaval varovanje brezžičnih omrežij, več poudarka na zagotavljanju varnosti na drugem OSI nivoju fizičnih omrežij, varnost pri zagotavljanju dostopa do storitev in omrežij v oblaku, varnost pri uporabi programsko definiranih omrežij ter upoštevanje protokola IPv6, ki ga je vedno več svetovnih organizacij zaradi pomanjkanja javnih IP naslovov protokola IPv4 primorano uporabljati že danes.

Na podlagi analize standarda ISO/IEC 27033 in sodobnih tehnik in tehnologije napadov potrjujem hipotezo, da zahteve in priporočila standarda ISO/IEC 27033 ne zagotavljajo dovolj učinkovitega varovanja komunikacijskih omrežij glede na najsodobnejše tehnike napadov, ki so prilagojene posamezni organizaciji.

LITERATURA IN VIRI

1. Akhgar, B., & Arabnia, H. (2013). *Emerging trends in ICT security*. Waltham: MK.
2. Andress, J. (2014). *The Basics of Information Security* (2nd ed.). Boston: Syngress.
3. Andress, J., & Winterfeld, S. (2014). *Cyber Warfare* (2nd ed.). Boston: Syngress.
4. Brewster, T. (2014, april). Protect your business by encrypting the network. Najdeno 22. junija 2015 na spletnem naslovu http://www.computerweekly.com/feature/Protect-your-business-by-encrypting-the-network
5. Cheng, T.-H., Lin, Y.-D., Lai, Y.-C., & Lin, P.-C. (2012). Evasion Techniques: Sneaking through Your Intrusion Detection/Prevention Systems. *Communications Surveys & Tutorials, IEEE, 14*(4), 1011-1020.
6. Chiacu, D., & Brunnstrom, D. (2014). State Department's unclassified email systems hacked. *Reuters.* Najdeno 13. junija 2015 na spletnem naslovu http://www.reuters.com/article/2014/11/17/us-cybersecurity-statedept-idUSKCN0J11BR20141117
7. *Codenomicon - Heartbleed bug*. Najdeno 3. aprila 2015 na spletnem naslovu http://heartbleed.com/
8. Cole, E. (2013). *Advanced Persistent Threat*. Boston: Syngress.
9. Daya, B. (2013). Network security: History, importance, and future. *University of Florida Department of Electrical and Computer Engineering.* Najdeno 10. junija 2015 na spletnem naslovu http://web.mit.edu/~bdaya/www/Network%20Security.pdf
10. Del Carlo, C. (2003). Intrusion detection evasion: How Attackers get past the burglar alarm. *SANS.* Najdeno 11. junija 2015 na spletnem naslovu http://www.sans.org/reading-room/whitepapers/detection/intrusion-detection-evasion-attackers-burglar-alarm-1284
11. Dela Torre, J., & Sioting, S. (2013). Network Detection Evasion Methods: Blending with Legitimate Traffic. *Trend Micro.* Najdeno 11. junija 2015 na spletnem naslovu http://speed.cis.nctu.edu.tw/~ydlin/pdf/Evasion_Techniques_Sneaking_through_Your_Intrusion_Detection_Prevention_Systems.pdf
12. Eckstein, C. (2014). Router backdoors - Can you trust your vendor? *SANS institute.* Najdeno 19. marca 2015 na spletnem naslovu http://www.giac.org/paper/gsec/26493/validating-security-configurations-detecting-backdoors-network-devices/122976
13. Gold, S. (2011). Advanced evasion techniques. *Network Security, 2011*(1), 16-19.
14. Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security, 5*(4), 438-457.
15. Gu, G., Zhang, J., & Lee, W. (2008). *BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic*. Atlanta, GA: Georgia Institute of Technology
16. Hayes, B. (2015). State Department Finally Cleans Malware From Emails Four Months After Hack. *Buzz Feed News.* Najdeno 13. junija 2015 na spletnem naslovu http://www.buzzfeed.com/hayesbrown/state-department-finally-cleans-malware-from-emails-four-mon#.yo55kyRXy
17. Hekmat, S. (2005). *Communication networks*. Newark, USA: PragSoft Corporation.
18. Internet Engineering Task Force - IETF. (1999). BGP/MPLS IP Virtual Private Networks (VPNs). Najdeno 10. marca 2015 na spletnem naslovu https://www.ietf.org/rfc/rfc4364.txt
19. Internet-Society. (2014). Global Internet Report 2014. Najdeno 25. februarja 2015 na spletnem naslovu http://www.internetsociety.org/sites/default/files/Global_Internet_Report_2014_0.pdf: Internet Society

20. ISACA. (2014). 2014 Advanced Persistent Threat Awareness. Najdeno 11. junija 2015 na spletnem naslovu www.isaca.org/Knowledge-Center/Research/Documents/APT-Survey-Report-2014_whp_Eng_0614.pdf
21. International Organization for Standardization - ISO. (b.l.). *ISO/IEC DIS 27033-6*. Najdeno 27. februarja 2015 na spletnem naslovu http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51585
22. International Organization for Standardization - ISO. (2009). ISO/IEC 27033-1:2009. *Information technology - Security techniques — Network security - Part 1: Overview and concepts.* Geneva: International Organization for Standardization (ISO).
23. International Organization for Standardization - ISO. (2010). ISO/IEC 27033-3:2010. *Information technology - Security techniques - Network security — Part 3: Reference networking scenarios - Threats, design techniques and control issues.* Geneva: International Organization for Standardization (ISO).
24. International Organization for Standardization - ISO. (2012). ISO/IEC 27033-2:2012. *Information technology - Security techniques - Network security — Part 2: Guidelines for the design and implementation of network security.* Geneva: International Organization for Standardization (ISO).
25. International Organization for Standardization - ISO. (2013a). ISO/IEC 27001:2013. *Information technology - Security techniques - Information security management systems - Requirements.* Geneva: Internationa Organization for Standardization (ISO).
26. International Organization for Standardization - ISO. (2013b). ISO/IEC 27002:2013. *Information technology - Security techniques - Code of practice for information security controls.* Geneva: International Organization for Standardization (ISO).
27. International Organization for Standardization - ISO. (2013c). ISO/IEC 27033-5:2013. *Information technology - Security techniques - Network security — Part 5: Securing communications across networks using Virtual Private Networks (VPNs).* Geneva: International Organization for Standardization (ISO).
28. International Organization for Standardization - ISO. (2014). ISO/IEC 27033-4:2014. *Information technology - Security techniques - Network security — Part 4: Securing communications between networks using security gateways.* Geneva: International Organization for Standardization (ISO)
29. Kartalopoulos, S. V. (2008). Differentiating Data Security and Network Security. *ICC '08. IEEE International Conference on Communications 2008* (str. 1469-1473), Tulsa: University of Oklahoma.
30. Kaspersky. (2015). Carbanak APT - The great bank robbery. Najdeno 31. marca 2015 na spletnem naslovu http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2015/02/Carbanak_APT_eng.pdf: Kaspersky LAB
31. Kershaw, M. (b.l.). Kismet Wireless. Najdeno 13. junija 2015 na spletnem naslovu https://www.kismetwireless.net/documentation.shtml
32. Kinger, P. (2015). Remembering the Vulnerabilities of 2014. Najdeno 24. marca 2015 na spletnem naslovu http://blog.trendmicro.com/trendlabs-security-intelligence/remembering-the-vulnerabilities-of-2014/
33. Lee, G. (2014). Chapter 8 - Storage Networks. In G. Lee (Ed.), *Cloud Networking* (str. 139-161). Boston: Morgan Kaufmann.
34. Lennon, M. (2015). Hackers Hit 100 Banks in 'Unprecedented' $1 Billion Cyber Heist: Kaspersky Lab. *Securityweek.* Najdeno 18. februarja 2015 na spletnem naslovu https://www.securityweek.com/hackers-hit-100-banks-unprecedented-1-billion-cyber-attack-kaspersky-lab
35. Lyon, G. (b.l.). NMAP Security Scanner. Najdeno 13. junija 2015 na spletnem naslovu https://nmap.org/

36. Martosko, D. (2015). State Department computer network goes dark after 'Russian' hackers infiltrate email systems. *Daily Mail.* Najdeno 13. junija 2015 na spletnem naslovu http://www.dailymail.co.uk/news/article-2994386/State-Department-computer-network-goes-dark-RUSSIAN-hackers-infiltrate-email-systems.html
37. McAfee. (2015). The Security Industry's Dirty Little Secret: The debate over advanced evasion techniques (AETs). Najdeno 12. junija 2015 na spletnem naslovu http://www.mcafee.com/us/resources/reports/rp-security-industry-dirty-little-secret.pdf
38. McClure, S., Scambray, J., & Kurtz, G. (2009). *Hacking exposed 6 : network security secrets & solutions*. New York: McGraw-Hill.
39. MITRE. (b.l.). Common Vulnerabilities and Exposures. Najdeno 19. marca 2015 na spletnem naslovu https://cve.mitre.org/
40. Möller, B., Duong, T., & Kotowicz, K. (2014). This POODLE Bites: Exploiting The SSL 3.0 Fallback. *Google.* Najdeno 3. aprila 2015 na spletnem naslovu https://www.openssl.org/~bodo/ssl-poodle.pdf
41. *April 2014 Web Server Survey. Netcraft.* Najdeno 3. aprila 2015 na spletnem naslovu http://news.netcraft.com/archives/2014/04/02/april-2014-web-server-survey.html
42. Niemi, O. P. (2013). [White Paper] Protect Against Advanced Evasion Techniques - Essential design principles. Najdeno 12. junija 2015 na spletnem naslovu http://www.mcafee.com/us/resources/white-papers/wp-protect-against-adv-evasion-techniques.pdf
43. NIST. (2013). *Security and privacy controls for federal information systems and organizations*. Najdeno 17. marca 2015 na spletnem naslovu http://permanent.access.gpo.gov/gpo28915/sp800-53-rev4-ipd.pdf
44. NIST. (2015). *National Vulnerability Database: Number of vulnerabilities in 2014*. Najdeno 19. marca 2015 na spletnem naslovu https://web.nvd.nist.gov/view/vuln/statistics-results
45. Pawar, M. V., & Anuradha, J. (2015). Network Security and Types of Attacks in Network. *Procedia Computer Science, 48*(0), 503-506.
46. Ptacek, T. H., & Newsham, T. N. (1998). *Insertion, evasion, and denial of service: Eluding network intrusion detection*: DTIC Document.
47. Reiske, W. (2014). *Shellshockernet*. Najdeno 3. aprila 2015 na spletnem naslovu https://shellshocker.net/
48. Roberts, P. (2014). *Infographic: A Heartbleed Disclosure Timeline (Secunia)*. Najdeno 4. aprila 2015 na spletnem naslovu https://securityledger.com/2014/06/infographic-a-heartbleed-disclosure-timeline-secunia/
49. Secunia. (2015). *Secunia Vulnerability Review 2015 Key figures and facts on vulnerabilities from a global information security perspective*. Nadeno 15. junija 2015 na spletnem naslovu http://secunia.com/?action=fetch&filename=secunia_vulnerability_review_2015_pdf.pdf
50. Tenable Network Security. (b.l.). *Nessus Vulnerability Scanner*. Najdeno 13. junija 2015 na spletnem naslovu http://www.tenable.com/products/nessus/features
51. Shakarian, P., Shakarian, J., & Ruef, A. (2013). *Introduction to Cyber-warfare*. Boston: Syngress.
52. SI-CERT. (2015). *Poročilo o omrežni varnosti za leto 2014*. Najdeno 15. junija 2015 na spletnem naslovu https://www.cert.si/wp-content/uploads/2015/05/Porocilo-o-omrezni-varnosti_2014.pdf: SI CERT.
53. Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information Security Management System Standards: A Comparative Study of the Big Five. *International Journal of Electrical & Computer Sciences, 11*(05), 21-27.

54. US-CERT. (2014). SSL 3.0 Protocol Vulnerability and POODLE Attack. Najdeno 1. aprila 2015 na spletnem naslovu US-CERT https://www.us-cert.gov/ncas/alerts/TA14-290A
55. Verizon. (2015). 2015 Data Breach Investigations Report. Najdeno 10. junija 2015 na spletnem naslovu http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015_en_xg.pdf
56. Weidman, G., & Eeckhoutte, P. V. (2014). *Penetration testing : a hands-on introduction to hacking*. San Francisco: No Starch Press.
57. Yadron, D. (2015). Three Months Later, State Department Hasn't Rooted Out Hackers. *The Wall Street Journal*. Najdeno 13. junija 2015 na spletnem naslovu http://www.wsj.com/articles/three-months-later-state-department-hasnt-rooted-out-hackers-1424391453
58. Younus, M. (2005). Wired 802.1x security. Najdeno 22. junija 2015 na spletnem naslovu http://www.sans.org/reading-room/whitepapers/networkdevs/wired-8021x-security-1654

PRILOGE

KAZALO PRILOG

Priloga 1: Terminološki slovar

802.1x	IEEE standard za overjanje omrežnih naprav na nivoju omrežnih vmesnikov.
Botnet omrežje	Več v omrežje povezanih računalnikov, nad katerimi napadalec prevzame nadzor, da bi jih uporabil za izvajanje zlonamernih dejanj.
Dvo/več domski prehod	angl: *Dual/Multi homed gateway*, omrežna naprava, ki povezuje omrežja, v katera ima priključne svoje fizične vmesnike.
Ranljivosti ničelnega dne	angl: *Zero day vulnerability*, s tem imenom označujemo ranljivosti na dan razkritja.
Razcepljeni tunel	angl: S*plit tunneling*, način medsebojnega povezovanja dveh naprav ali omrežij z uporabo tunela, kjer promet med napravami ali omrežji usmerjamo preko tunela, preostali promet pa preko privzetega prehoda.

Priloga 2: Krajšave

BGP	angl: *Border Gateway Protocol*, zunanji usmerjevalni protokol za izmenjavo usmerjevalnih tabel med različnimi avtonomimi sistemi.
DNSSEC	angl: *Domain Name Server Security Extensions*, protokolna dopolnila za varno razreševanje domenskih imen in izmenjavo domenskih zapisov.
FC	angl: *Fibre Channel*, protokol za blokovno izmenjevanje podatkov med napravami.
FCoE	angl: *Fibre Channel over Ethernet*, protokol za blokovno izmenjevanje podatkov med napravami preko ethernet protokola.
IDS	angl: *Intrusion Detection System*, sistemi za zaznavanje napadov.
IPS	angl: *Intrusion Prevention System*, sistemi za preprečevanje napadov.
IPSEC	angl: *IP Security*, protokol za varno izmenjavo podatkov z uporabo šifriranja in overjanje.
iSCSI	angl: *Internet Small Computer System Interface*, protokol za blokovno izmenjavo podatkov preko IP omrežij.
MACSec	angl: *Media Access Control Security protokol*, protokol za šifriranje podatkov na 2. OSI nivoju.
MPLS	angl: *Multiprotocol Label Switching*, protokol, ki omogoča prenos paketov različnih protokolov preko omrežja z uporabo oznak.
SAN	angl: *Storage Area Network*, namensko omrežje, ki omogoča dostop do skupnega blokovnega pomnilniškega medija.
SSL	angl: *Secure Socket Layer*, protokol za šifriranje povezave med odjemalcem in strežnikom.
UTM	angl: *Unified Threat Management*, naprava, ki evolucijsko nadomešča požarne pregrade in vsebuje napredne varnostne funkcije.