Centar Informacijske Sigurnosti

Defense in depth

svibanj 2012.

CIS-DOC-2012-05-050

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

9. REFERENCE **24**

1. Uvod

Strategija Defense in depth već dugo je prisutna u stvarnom svijetu. Poznati povijesni zapisi kažu kako se prvi put koristila u bitci kod Cannae 216 godina p.n.e. Ovom strategijom se raspoređuju vojni resursi obrane te se napadačima lako predaje dio teritorija. Kako napadači napreduju kroz teritorij, obrane stalno nailaze na prepreke te su svakim prolaskom kroz prepreku slabiji. Ulaskom napadača na teritorij obrane, napadači se postavljaju u lošiju poziciju gdje ih se može napasti s više strana, a i svakim napredovanjem oni slabe. Opisana strategija se pokušala prenijeti i u virtualni, odnosno računalni svijet kako bi se spriječili napadači i zlonamjerni korisnici. U računalnom okruženju stvoreni su višestruki slojevi obrane kroz cijeli sustav informacijske tehnologije. Glavni cilj je stvoriti redundanciju u obrani kako bi se održala sigurnost sustava ako sigurnosna provjera ne uspije ili se iskoristi ranjivost sustava. Prilikom obrane računalnih mreža strategija Defense in depth trebala bi spriječiti ugrožavanje sigurnosti, ali i omogućiti dodatno vrijeme kako bi se moglo reagirati na napad. Kako bi se postigla zaštita informacija, treba biti uravnotežena usmjerenost na tri glavna elementa: korisnike, tehnologiju i radnje. Više informacija nalazi se u trećem poglavlju ovog dokumenta. U četvrtom poglavlju je opisano kako se strategija Defense in depth koristi u informacijskoj sigurnosti. Prilikom projektiranja ove slojevite strategije mogu se mijenjati parametre svake razine kako bi se strategija prilagodila sigurnosnim prioritetima i potrebama određene organizacije. Razine strategije su: razina podataka, razina za primjenu, razina računala, razina unutarnje mreže, razina periferne mreže, razina fizičke sigurnosti te razina pravila, procedura i svijesti. Peto poglavlje opisuje prednosti i nedostatke ove strategije, dok su u šestom poglavlju opisani drugi sigurnosni principi s kojima se strategija Defense in depth može usporediti.

2. Strategija Defense in depth u vojsci

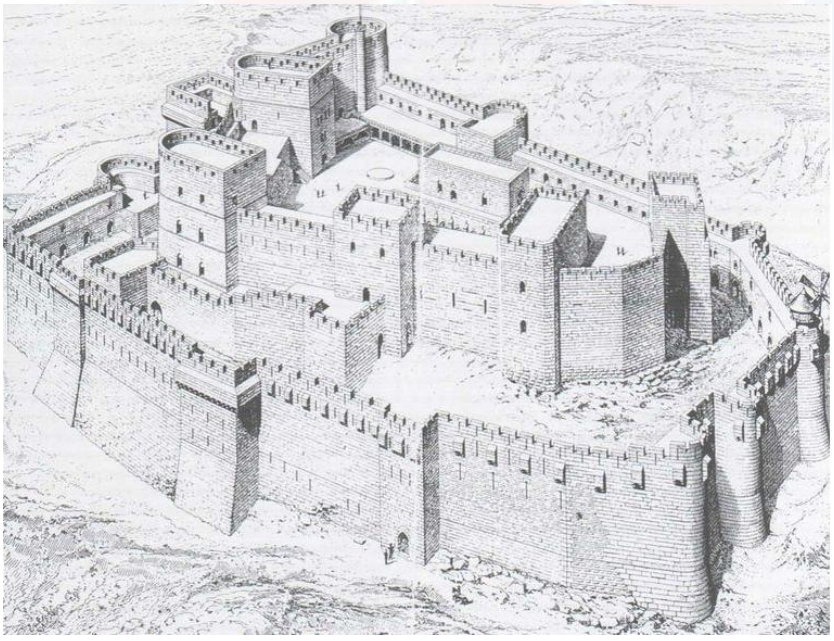
Konvencionalna strategija obrane je ona koja postavlja sve vojne resurse na prvu liniju te ako dođe do proboja napadača preostali branitelji bili bi ugroženi jer bi ih se moglo zaobići i okružiti. Ovim načinom bi linije za komunikaciju i zapovijedanje mogle postati ranjive.

Strategija Defense in depth zahtjeva raspoređivanje vojnih resursa obrane, primjerice u utvrde, na terenske radove i na kraju u vojne jedinice koje su jako daleko od prve linije. Iako napadač možda misli kako je lakše probiti oslabljenu prvu obrambenu liniju, kako napreduje prema naprijed neprestano nailazi na otpor. Kako se napadač probija dublje u obrambene redove, krajnji dijelovi njegovog napada postaju ranjivi te na taj način riskira jer se može dogoditi da ga okruže. Ova strategija posebno je djelotvorna protiv napadača koji nije u stanju usmjeriti svoje snage i napasti mali broj mjesta na proširenoj obrambenoj liniji.

Branitelji koji se mogu vratiti na uzastopno pripremljene pozicije mogu postići veliki dobitak kada neprijatelj napreduje dok izbjegava opasnost pa ga se tada može prijeći ili zaobići. Odgađanje napretka neprijatelja ublažava prednost napadača koju bi imao s efektom iznenađenja te omogućauje dodatno vrijeme za preseljenje obrambenih jedinica kako bi posložili obranu i pripremili protunapad.

Dobro isplanirana strategija Defense in depth rasporedit će vojne snage na pozicije koje si međusobno pomažu te će im dati odgovarajuće uloge. Primjerice, loše obučene postrojbe mogu se rasporediti u statičku obranu na prvoj linije, dok bolje obučene i opremljene postrojbe čine mobilnu rezervu. Uspješni slojevi obrane mogu koristiti različite tehnologije i taktike. Primjerice red pod nazivom zubi zmaja (eng. *dragon's teeth*) može biti problem za tenkove, ali nije prepreka za pješaštvo, dok neka druga barijera od žice ima suprotan efekt. Strategija Defense in depth omogućuje braniteljima najviše povećavanje obrambenih mogućnosti prirodnog terena i druge prednosti.

Braniteljima može biti neprihvatljivo isplanirati prepuštanje terena napadačima i to je jedan od nedostataka strategije Defense in depth. To se može dogoditi zbog toga što su značajni vojni i ekonomski resursi preblizu prednjoj liniji ili jer je popuštanje neprijateljima neprihvatljivo iz političkih ili kulturalnih razloga. Osim toga, za neprekinuto povlačenje koje zahtjeva ova strategija branitelji trebaju imati veliki stupanj mobilnosti kako bi se uspješno mogli povući te trebaju imati visoki moral kako bi se mogli oporaviti od poraza. Na Slika 1 nalazi se prikaz dvorca u Siriji koji je primjer strategije Defense in depth [6].



Slika 1. Prikaz dvorca u Siriji koji se zove „Krak des Chevaliers"
Izvor: Wikipedia

2.1. Primjeri strategije Defense in depth

Rani primjer strategije Defense in depth mogao se vidjeti u bitci kod Cannae 216 godina p.n.e. kada je Hanibal izveo manevar kako bi okružio i odjednom uništio 10 rimskih legija. Rezultat ovoga je najveći poraz rimskih trupa u povijesti republike.

Kasniji primjeri strategije Defense in depth mogle bi biti europske utvrde na vrhovima planina (brda) i razvoj koncentričnih dvoraca. U ovim primjerima, unutarnji slojevi obrane mogu podržati vanjske slojeve s vatrenim strijelama i napadač mora proći svaku liniju obrane i preživjeti moguće značajne gubitke dok branitelji imaju mogućnost povratka u napad. U američkom revolucionarnom ratu i bitci Cowpens, američke snage bile su smještene u tri linije koje su ublažile šok od britanskog naleta koji su im nanijeli veliku štetu prije nego što su uspjeli osvojiti Britance, koji su u tom trenutku izgubili međusobnu povezanost.

Noviji primjeri strategije Defense in depth uključuju višestruke linije obrane u Prvom svjetsko ratu koje su isplanirane za obranu Velike Britanije koja je bila pod prijetnjom njemačke invazije. Tijekom bitke za Normandiju, njemačke oružane snage pod nazivom Wehrmacht koriste malu šumu u području kako bi stvorile uzastopne linije obrane koje su usporile napade saveznika i produžile vrijeme za dolazak pojačanja. Bitka koja se odvijala na Pacifiku u Drugom svjetskom ratu ima puno primjera strategije Defense in depth i tada su Japanci nanijeli teške gubitke Amerikancima u bitkama Tarawa, Saipan, Peleliu, Iwo Jima i Okinawa. Pukovnik Francis J. Kelly raspravlja o uporabi strategije Defense in depth zapovjednicima u logorima specijalnih vojnih snaga tijekom američkog sudjelovanja u ratu u Vijetnamu. Kelly je bivši zapovjednik specijalnih vojnih snaga u SAD-u i autor knjige „Vietnam studies U.S. army special forces 1961.-1971.“ Objasnio je kako su kampovi specijalnih jedinica bili vrlo funkcionalni i lako branjivi [7].

3. Primjena strategije u informacijskoj sigurnosti

Strategija Defense in depth djeluje dobro u stvarnom svijetu jer se mogu primijeniti zakoni fizike, ali i zato jer osoba ne može jednostavno samo proći kroz čvrstu prepreku. U računalnom svijetu ništa nije stvarno te tako nije bitno nalazili li se neprijatelj u blizini svog cilja ili je na drugom kraju svijeta. Računalni svijet ima zakone, ali oni su različiti od fizikalnih zakona za koje je strategija prvotno osmišljena te to zlonamjerni korisnici iskorištavaju.

Strategija Defense in depth koristi se za postizanje informatičke sigurnosti u današnjem jako umreženom okruženju. Najviše se koristi zbog toga što se oslanja na inteligentnu primjenu tehnika i tehnologija koja danas postoje. Strategija preporuča ravnotežu između sposobnosti zaštite i cijene, učinkovitosti i operativnih razmatranja.

Strategija Defense in depth je koncept informacijskog osiguranja u kojem su višestruki slojevi za provjeru sigurnosti (obranu) smješteni kroz cijeli sustav informacijske tehnologije[1] (eng. *Information Technology*, IT). Svrha ovog koncepta obrane je pružanje redundancije u slučaju ako sigurnosna provjera ne uspije ili ako bude iskorištena ranjivost sustava. Mogu se iskoristiti ranjivosti osoblja te proceduralne, tehničke i fizičke ranjivosti. Glavna ideja strategije je štiti sustav protiv nepoznatih napada korištenjem nekoliko različitih metoda. To je taktika koja se dijeli na slojeve, a prva ju je osmislila nacionalna sigurnosna agencija SAD-a (eng. *National Security Agency*, NSA) kao sveobuhvatni pristup informacijskoj i elektroničkoj sigurnosti.

Kao što je navedeno u drugom poglavlju strategija Defense in depth izvorno je vojna strategija koja pokušava odgoditi (umjesto spriječiti), napredovanje napadača tako da im predaje teren kako bi dobili na vremenu. Postavljanjem zaštitnih mehanizama, procedura i pravila pokušava se povećati pouzdanost nekog IT sustava gdje višestruki slojevi obrane sprječavaju motrenje i izravne napade na kritične sustave. U pogledu obrane računalnih mreža, strategija Defense in depth ne bi trebala samo spriječiti narušavanje sigurnosti, nego omogućiti dodatno vrijeme koje je potrebno za reagiranje na napad te na taj način smanjiti i ublažiti posljedice narušavanja sigurnosti.

Poduzećima i stručnjacima sigurnosti informacijske tehnologije trebalo je jako puno vremena, novaca i sredstava kako bi razvili pristup strategije Defense in depth u sigurnosti informacijske tehnologije. Ipak, uspješni napadi na mnoge tvrtke (RSA, HB Gary Booz, Allen & Hamilton, vojska SAD-a) primjer su neodrživosti strategije Defense in depth u praksi jer se neprijatelji (napadači) ne mogu u potpunosti ukloniti. Bolje razmatranje razvoja strategije i načina na koji je napravljena kako bi se uklopila u informacijske tehnologije vrlo je važno kako bi se shvatili današnji trendovi. Znajući kako strategija Defense in depth čini organizacije ranjivijima bitno je razumjeti kako je potrebna promjena u stavovima i mišljenju za bolje rješavanje rizika s kojima se suočavaju na učinkovitiji način. Osiguravanje informacija više je od same sigurnosti računalnog sustava. To je skup metoda, tehnika, alata, ljudi i procesa koji su potrebni za zaštitu informacija. Informacije su kritično sredstvo u vladama, poduzećima i organizacijama koje se zasnivaju na informacijama te su o njima ovisne.

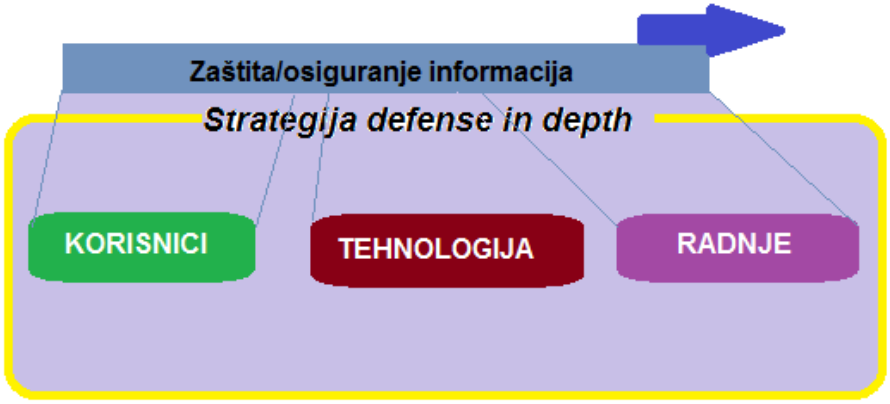
Za učinkovito odupiranje napadima na informacije i informacijske sustave, organizacija treba opisati i karakterizirati svoje protivnike, njihovu moguću motivaciju te njihove klase napada. Potencijalni protivnici mogu uključivati: nacionalne zemlje, teroriste, kriminalne elemente, napadače ili korporativne konkurente. Njihova motivacija može uključivati: prikupljanje osjetljivih podataka, napad uskraćivanjem usluge (eng. *Denial of Service* - DoS), nelagodu ili ponos zbog iskorištavanja značajnog cilja. Kategorije napada mogu uključivati: pasivno nadziranje komunikacija, aktivne napade na mrežu, napade iz neposredne blizine, iskorištavanje zaposlenika te napade putem onih koji daju nečija sredstva informacijske tehnologije. Važno je oduprijeti se štetnim učincima događaja koji nisu zlonamjerni kao što su vatra, poplava, nestanak struje i pogreške korisnika.

3.1. Osiguravanje informacija

Osiguravanje informacija postiže se kada su informacije i informacijski sustavi sigurni i zaštićeni protiv napada putem primjene sigurnosnih usluga kao što su: dostupnost, cjelovitost,

[1] Informacijska tehnologija (eng. *Information Technology* - IT) je tehnologija koja koristi računala za prikupljanje, obradu, pohranu, zaštitu i prijenos informacija. Terminu IT su pridružene komunikacijske tehnologije jer je danas rad s računalom nezamisliv ako ono nije povezano u mrežu pa se govori o informacijskoj i komunikacijskoj tehnologiji (engl. *Information and Communications Technology - ICT*).

autentičnost, povjerljivost i nepriznavanje. Primjena ovih usluga trebala bi se zasnivati na paradigmi: zaštiti, otkrij i reagiraj (eng. *Protect, Detect and React*). To znači kako uz uključivanje mehanizama zaštite, organizacije trebaju očekivati napade te uključiti alate za otkrivanje napada i procedura koje će im omogućiti djelovanje i oporavljanje od napada. Važan princip strategije Defense in depth je u tome što postizanje zaštite informacija zahtjeva uravnoteženu usmjerenost na tri glavna elementa: korisnike, tehnologiju i radnje, a prikaz se nalazi na Slika 2.



Slika 2. Zaštita informacija
Izvor: Defense in depth

3.1.1. Korisnici

Postizanje informacijske sigurnosti počinje s više razina upravljanja obvezama, a zasniva se na razumijevanju percipirane prijetnje. To se mora pratiti s učinkovitim pravilima i procedurama zaštite informacija, raspodjelom uloga i odgovornosti, predanosti sredstava, obukom ključnog osoblja (korisnici i administratori sustava) te osobnim odgovornostima. Moraju se uspostaviti mjere fizičke i osobne sigurnosti kako bi se provjeravao i nadzirao pristup ustanovama i kritičnim elementima okruženja informacijske tehnologije.

3.1.2. Tehnologija

Danas je dostupan širok raspon tehnologija za pružanje usluga informacijske sigurnosti te za otkrivanje upada (eng. *Intrusion Detection*) u sustav. Kako bi se organizacije osigurale da kupuju i koriste prave tehnologije, trebaju uspostaviti učinkovita pravila i postupke za kupnju novih tehnologija. To uključuje: sigurnosna pravila, principe za osiguranje informacija, arhitekture i standarde za razine sustava zaštite informacija, kriterije za potrebne proizvode za zaštitu informacija, nabavku proizvoda koje su drugi isprobali i potvrdili njihovu kvalitetu, upute za konfiguraciju i postupke za procjenu rizika integriranih sustava. Strategija Defense in depth preporuča nekoliko principa za osiguranje informacija, a to su:

1. Obrana s više mjesta – Obzirom da protivnici mogu napasti cilj iz više točaka, organizacija mora rasporediti mehanizme za zaštitu na višestruke različite lokacije kako bi se mogla obraniti od svih vrsta napada. Najmanje što obrambena područja trebaju sadržavati je:
    - obrana mreže i infrastrukture – Zaštita lokalne i širokopojasne komunikacijske mreže (primjerice od napada uskraćivanjem usluga). Pružanje povjerljivosti i cjelovite zaštite za podatke koji se prenose putem tih mreža (primjerice treba koristiti šifriranje i sigurnosne mjere za tok prometa kako bi se korisnici mogli obraniti od pasivnog nadziranja),

- treba braniti granice - primjer je primjena vatrozida (eng. *firewall*) i otkrivanje upada[2] kako bi se mogli obraniti od aktivnih napada na mrežu,
- obrana računalnog okoliša - npr. pružanje provjere pristupa računalima i poslužiteljima za obranu od napada iznutra, napada iz neposredne blizine i distribuiranih napada.

2. Slojevita obrana – Čak i najbolji dostupni proizvodi za zaštitu informacija imaju slabosti, stoga je samo pitanje vremena kada će neki protivnik pronaći ranjivost koju može iskoristiti. Učinkovita protumjera je primjena višestrukih mehanizama za obranu koji se nalaze između protivnika i njegovog cilja. Svaki od ovih mehanizama mora predstavljati jedinstvenu prepreku napadaču te bi svaki trebao biti u mogućnosti zaštiti i otkriti protivnike. Na taj način povećava se rizik (otkrivanja) za napadača dok se smanjuju njegove mogućnosti za uspjeh. Postavljanje vatrozida (zajedno s otkrivanjem upada u sustav) na vanjske i unutarnje mrežne granice primjer je slojevite obrane. Unutarnji vatrozid može podržavati precizniju provjeru pristupa i filtriranje podataka.
3. Određivanje robusnosti sigurnosti (snaga i osiguranje) za svaku komponentu zaštite informacija u zavisnosti od vrijednosti onoga što se štiti i prijetnji u trenutku primjene. Primjerice, često je učinkovitije i pogodnije rasporediti jače mehanizme na rubove mreže nego na radnu površinu korisnika.
4. Treba uvesti snažno ključno upravljanje i infrastrukture s javnim ključem koje podržavaju sve ugrađene tehnologije za zaštitu informacija te su vrlo otporne na napade.
5. Uvođenje infrastrukture za otkrivanje upada u sustav i za analizu i korelaciju rezultata te kako bi se moglo reagirati sukladno s tim. Spomenuta infrastruktura trebala bi pomagati djelatnicima koji obrađuju podatke kako bi odgovorili na sljedeća pitanja: Nalazi li se mreža pod napadom? Tko je izvor napada? Što je tema napada? Tko je sve pod napadom? Koje su mogućnosti u borbi protiv napada?

3.1.3. Radnje

Radnje, usmjerene na sve aktivnosti koje su potrebne kako bi se (iz dana u dan) zadržala sigurnost organizacije uključuju:

1. Održavanje vidljivih i ažuriranih pravila sigurnosti sustava.
2. Certifikaciju i akreditaciju primjena referentnih informacijskih tehnologija - ovaj bi proces trebao omogućiti podatke za podršku upravljanja rizikom koja se zasniva na odlukama. Procesima bi trebalo biti poznato da ako jedan korisnik prihvati rizik to je onda rizik koji svi u organizaciji dijele.
3. Upravljanje sigurnosnim pravilima tehnologije za zaštitu informacija (npr. instalacija sigurnosnih nadogradnji, nadogradnja baze podataka antivirusa, održavanje liste provjere pristupa).
4. Pružanje ključnih usluga upravljanja i zaštita ovakve infrastrukture.
5. Obavljanje zadataka za sigurnost sustava (npr. pretraživanje ranjivosti) kako bi se procijenila stalna spremnost sigurnosnog sustava.
6. Nadziranje i reakcija na trenutne prijetnje.
7. Očitavanje napada, upozorenje i reagiranje.
8. Oporavak i rekonstrukcija.

[2] Sustav za otkrivanje upada je uređaj ili program koji nadzire aktivnosti na mreži ili u sustavu i traži zlonamjerne aktivnosti ili kršenje pravila.

3.1.4. Dodatna sredstva

Nacionalna agencija za sigurnost s podrškom agencija vlade SAD-a i njihove industrije poduzela je niz inicijativa kako bi podržala strategiju Defense in depth. Spomenute inicijative uključuju:

1. Tehnički radni okvir za zaštitu informacija – U dokumentu na web stranici:

https://www.iad.gov/library/iacf.cfm

nalaze se detaljne upute za osiguranje informacija za svako područje strategije Defense in depth.

2. Nacionalno partnerstvo za informacijsko osiguranje[3] (eng. *National Information Assurance Partnership,* NIAP) - partnerstvo između NSA-e i Nacionalnog instituta za standarde i tehnologiju (eng. *National Institute of Standards and TechnologyI,* NIST) kako bi potaknuli razvoj međunarodnog zajedničkog kriterija (eng. *International Organization for Standardization,* ISO) te kako bi akreditirali komercijalne laboratorije za provjeru sigurnosti proizvoda.
3. Profili općih kriterija za zaštitu – dokumenti koji preporučuju sigurnosne funkcije i razine osiguranja koristeći Opće Kriterije. Dostupni su za široki raspon komercijalno dostupnih tehnologija i može im se pristupiti na web stranici organizacije NIAP.
4. Popis ocijenjenih proizvoda – popis komercijalnih proizvoda za osiguranje informacija koji su procijenjeni prema Općem kriteriju. Popis održava organizacija NIST te su dostupni na web stranicama organizacije NIAP.
5. Upute za konfiguraciju – dokumente je pripremila agencija NSA, a sadrže preporučene konfiguracije za različite često korištene komercijalne proizvode.

Rječnik pojmova – rječnik organizacije Nacionalna sigurnost informacijskih sustava (eng. National Information Systems Security, INFOSEC) [2] može se naći na web stranici:

http://www.nstissc.gov/Assets/pdf/4 009.pdf.

[3] Nacionalno partnerstvo za informacijsko osiguranje (eng. *National Information Assurance Partnership,* NIAP) inicijativa je vlade SAD-a kako bi se zadovoljile potrebe sigurnosnih testiranja korisnika informacijske tehnologije i proizvođača kojima upravlja Agencija za nacionalnu sigurnost. Agencija NIAP zajednički je pothvat Agencije za nacionalnu sigurnost i Nacionalnog instituta za standarde i tehnologiju.

4. Opis strategije i primjena u informacijskoj sigurnosti

Sve organizacije trebale bi razviti antivirusna rješenja koja pružaju visoki stupanj zaštite. Međutim, čak i nakon instalacije antivirusnih programa, organizacije je još uvijek moguće napasti i zaraziti njihova računala i mreže. Zajedno s projektom za mrežnu sigurnost tvrtka Microsoft preporuča pristup Defense in depth za antivirusno rješenje kako bi se osigurala zaštita organizacija pomoću antivirusnih programa. Ovakav pristup je vrlo važan u računalnoj sigurnosti organizacije jer bez obzira koliko računalni sustav nudi sigurnosnih mogućnosti ili usluga netko će pokušati pronaći ranjivost kakao bi je iskoristio u zlonamjerne svrhe. Cilj ovog pristupa je razumjeti svaku razinu modela i određene prijetnje koje odgovaraju svakoj razini kako bi mogli koristiti informacije pri primjeni antivirusnog rješenja.

Jednom kada se otkriju i dokumentiraju rizici s kojima se organizacija suočava treba proučiti i napraviti obranu koja će se koristiti kao antivirusno rješenje. Sigurnosni model Defense in depth definira sedam razina sigurnosnih obrana koje su osmišljene kako bi osigurale da napadi koji ugrožavaju sigurnost organizacije naiđu na robustan skup obrana. Svaki skup sposoban je odbiti napad na puno različitih razina.

Slojevi koji su prikazani Slika 33 pružaju pogled na svako područje u okolini neke tvrtke koje treba razmotriti pri projektiranju sigurnosne obrane za mrežu neke organizacije.

Slika 3. Prikaz razina definiranih za sigurnosni model Defense in depth
Izvor: The Antivirus Defense-in-Depth Guide

Pri projektiranju mogu se mijenjati detaljne definicije svake razine s obzirom na sigurnosne prioritete i potrebe određene organizacije. Sljedeće jednostavne definicije koje se nalaze u poglavljima od 4.1. do 4.7. određuju razine ovog modela.

Korištenje sigurnosnih razina modela kao osnova za antivirusni pristup Defense in depth omogućuje preusmjeravanje pogleda kako bi ih optimizirali u skupine za antivirusnu obranu u određenoj organizaciji. Kako se optimizacija prikazuje u određenoj organizaciji, potpuno ovisi o prioritetima organizacije te specifičnim programima koji se koriste za antivirusnu obranu. Vrlo je važno izbjeći nepotpuno ili oslabljeno konstruiranje antivirusne obrane tako da se sve sigurnosne razine uključe u obranu [8].

4.1. Razina podataka

Rizici na razini podataka dolaze iz ranjivosti koje napadač može iskoristiti za dobivanje pristupa konfiguracijskim podacima, organizacijskim podacima ili bilo kojoj vrsti podataka koji su jedinstveni za uređaj koji organizacija koristi. Primjerice, osjetljive podatke kao što su povjerljivi poslovni podaci, korisnički podaci ili privatne informacije o kupcima. Primarna briga za organizaciju na ovoj razini modela su poslovni i pravni problemi koji mogu nastati zbog gubitaka podataka ili krađe te radni problemi koje ranjivosti mogu izložiti na računalnoj razini ili razini za primjenu.

4.2. Razina za primjenu

Rizik na razini za primjenu dolazi iz ranjivosti koje bi napadač mogao iskoristiti pristupom aplikacijama koje su pokrenute. Bilo koji izvršni kod koji zlonamjerni programer može koristiti izvan operacijskog sustava može se iskoristiti za napad na sustav. Glavna zabrinutost za organizaciju na ovoj razini je pristup binarnim datotekama koje dolaze od aplikacija, pristup računalu putem ranjivosti u uslugama za nadziranje aplikacija ili neprimjereno prikupljanje određenih podataka iz sustava kako bi se zaobišao netko tko ih može iskoristiti u vlastite svrhe.

4.3. Razina računala

Ova razina obično je na meti onih koji daju pakete usluga i brze popravke kako bi riješili zlonamjerne prijetnje. Rizici na ovom sloju nastaju od napadača koji iskorištavaju ranjivosti u uslugama koje nude računala ili uređaji. Napadači iskorištavaju te ranjivosti na razne načine kako bi napravili napade protiv sustava. Do preljeva međuspremnika (eng. *buffer overflow*) dolazi zbog dodavanja previše informacija međuspremniku. Glavna briga za organizaciju na ovoj razini je sprječavanje pristupa binarnim datotekama koje čine operacijski sustav kao i pristup računalu putem ranjivosti u uslugama za prisluškivanje operacijskog sustava.

4.4. Razina unutarnje mreže

Rizici za unutarnju mrežu organizacije uglavnom se odnose na osjetljive podatke koji se prenose mrežama ovog tipa. Zahtjevi povezanosti radnih stanica klijenta s ovim unutarnjim mrežama također donose određene rizike.

4.5. Razina periferne mreže

Rizici povezani s perifernim mrežama dolaze od napadača koji su dobili pristup mrežama širokog područja i razini mreže na koju se spajaju. Glavni rizici na ovoj razini usmjereni su na dostupne priključnice protokola TCP (eng. *Transmission Control Protocol*) i UDP (eng. *User Datagram Protocol*) koje se koriste u mreži.

4.6. Razina fizičke sigurnosti

Rizici na ovoj razini dolaze od napadača koji imaju fizički pristup fizičkoj imovini organizacije. Ovaj sloj obuhvaća sve prethodne razine jer ako napadač ima fizički pristup imovini može si omogućiti pristup svim ostalim razinama u modelu Defense in depth. Glavna zabrinutost na ovoj razini modela za organizaciju koja koristi antivirusni sustav je zaustaviti zaražene datoteke da zaobilaze obranu periferne i unutarnje mreže. Napadači ovo mogu pokušati napraviti jednostavnim kopiranjem zaraženih datoteka izravno u računalo putem fizičkih prijenosnih medija, kao što je uređaj USB (eng. *Universal Serial Bus*).

4.7. Razina pravila, procedura i svijesti

Obuhvaćanjem svih razina sigurnosnog modela su pravila i procedure koje određena organizacija treba postaviti kako bi zadovoljila i podržala zahtjeve za svaku razinu. Vrlo je važno za organizaciju promicanje svijesti svim zainteresiranim stranama. U mnogim slučajevima, ignoriranje rizika može dovesti do sigurnosnog propusta te bi iz tog razloga obuka trebala biti sastavni dio svakog sigurnosnog modela.

Prednosti i nedostaci strategije Defense in depth

Strategija Defense in depth razvijena je kako bi zaštitila kinetički ili stvarni svijet, vojnu ili stratešku imovinu stvaranjem slojeva obrane. Napadači zbog slojevite obrane moraju proširiti većinu svojih resursa dok proširuju liniju za opskrbu. Taktički cilj je odgoditi i učiniti neprijateljski napad neodrživim. Rezultat strategije je to što napadač postaje ranjiv na protunapad. Branitelji tada imaju mogućnost protunapada te uklanjanje prijetnje. U kinetičkom svijetu gradijent gubitka snage (eng. *Loss of Strength Gradient*, LSG) ključni je pokazatelj učinkovitosti strategije Defense in depth. On pokazuje da što je napadač udaljeniji od svog cilja to mu manje snage može biti dostupno. Geografska udaljenost nevažna je u računalnoj obrani. Napadači mogu biti na suprotnoj strani planete i biti učinkoviti kao da sjede odmah pored cilja napada. Mnogi napadači su imuni na djelovanje zakona zbog ograničenja međudržavnih granica i manjka zakona koji se provode ili čak i ne postoje ti zakoni koji bi zaustavili takve zlonamjerne aktivnosti.

Strategija Defense in depth u svom izvornom konceptu djeluje za obranu stvarnog svijeta. Problem strategije u obrani računalnog svijeta je što je neodrživa. Stručnjaci za sigurnost informacijske tehnologije koriste komponentu strategije Defense in depth koja se naziva „Slojevita obrana“[4] (eng. *Layered Defense*). Strategiji Defense in depth potrebna je slojevita obrana, ali ako korisnik ima samo slojevitu obranu to ne ispunjava zahtjeve strategije Defense in depth kao cjeline. Ono što se koristi u civilnom sektoru ne može se nazvati strategijom Defense in depth jer oni ne mogu ispuniti izvornu namjenu strategije i protunapad kako bi uništili protivnika. Protunapad nije legalan te bi moral protunapada bio upitan. Računalni svijet prepun je anomalija, propusta, pogrešaka i ranjivosti koje omogućuju napadaču maskiranje prometa te ga čak može učiniti i potpuno nevidljivim.

Dokazi uspješnih napada pokazuju propuste strategije Defense in depth, a to su:

- povećava se broj uspješnih napada,
- povećava se učestalost uspješnih napada,
- trud koji je potrebno uložiti za uspješan napad se smanjuje,
- smanjuje se razina znanja potrebna za uspješan napad.

Uzimajući u obzir smanjenje primjene strategije Defense in depth u informacijskoj sigurnosti te kako je strategija dospjela u informacijsku tehnologiju pokazuje se kako se stalno smanjuje broj uspješnih napada kako se strategija razvija. Mogućnost sprječavanja svih pokušaja napada na mrežu je nemoguća. Nije bitno koje mjere su poduzete ukoliko su napadači dovoljno uporni jer će tako uspjeti zaobići sigurnosne sustave.

Prednost strategije je što se sastoji od puno slojeva obrane koji svi zajedno pridonose cjelovitoj sigurnosti sustava. Ukoliko napadač uspije iskoristiti ranjivosti jednog sloja ili uspije zaobići sigurnosne sustave i tehnike na tom sloju preostaju drugi komplementarni slojevi koji mogu spriječiti napad [1].

[4] Slojevita obrana (eng. *Layered Defense*) se koristi kako bi se opisao sigurnosni sustav koji je napravljen korištenjem različitih alata i pravila kako bi zaštitio višestruka područja u mreži od različitih prijetnji uključujući računalne viruse, krađu, nedozvoljene pristupe i druge.

5. Usporedba s drugim sigurnosnim principima

U ovom poglavlju bit će opisani i drugi sigurnosni principi pa se mogu usporediti s principom Defense in depth.

5.1. Etika u sigurnom razvoju programa

Organizacije za razvoj programa trebale bi se ponašati etički u cjelini, ali ne bi trebale očekivati kako će njihove pojedine komponente to biti. Etički je ne izlagati korisnika sigurnosnim rizicima koji su poznati. Također, etički je dati korisnicima određena pravila privatnosti kada koriste svoje osobne informacije kako bi mogli djelovati i izbjeći nepoželjno korištenje takvih informacija. Osim toga, ako organizacija promijeni pravila privatnosti korisnik bi trebao imati mogućnost izbora prihvatiti promjene ili izbrisati svoje osobne podatke. Ukoliko organizacija ima ugroženi sustav na kojem se nalaze podaci korisnika, etički je obavijestiti korisnika o povredi privatnosti.

5.2. Unutarnje prijetnje su kao slaba karika

Većina organizacija za razvoj programa predvidi unutarnje rizike, primjerice rizik koji stvaraju korisnici koji imaju pristup aplikacijama unutar organizacije. Na primjer, pri planiranju implementacije najlakše je pretpostaviti kako je vatrozid tu i ne brinuti se, iako postoje mnoge tehnike za zaobilaženje vatrozida. Većina organizacija u potpunosti ignorira rizike kolega koji su do njih, tajnika i domara te rizik od onih koji su nedavno dali otkaz ili su ga dobili. Ne bi se trebalo vjerovati svim korisnicima koji se nalaze unutar organizacije. Ne mora biti kako su zaposlenici organizacije nezadovoljni ili ih je lako podmititi, možda su oni samo slučajno odali informacije jer su postali žrtvom napada socijalnog inženjeringa (eng. *social engineering*). Socijalni inženjering je kada napadač koristi svoje socijalne vještine (najčešće uključuje prijevaru) kako bi ostvario svoje sigurnosne ciljeve. Primjerice, takav napadač mogao bi uvjeriti tehničku podršku kako je on stvarni korisnik koji je zaboravio svoju lozinku pa mu korisnička podrška oda korisnikove podatke.

5.3. Pretpostavka kako je mreža ugrožena

Postoji puno kategorija napada koje mogu pokrenuti napadači s pristupom bilo kojem mrežnom mediju koji može vidjeti web promet aplikacije. Najveći rizik nalazi se u lokalnim mrežama koje koriste krajnji korisnici. Puno korisnika misli kako će uključivanje u mrežu putem priključnice spriječiti prijetnje u lokalnoj mreži. Nažalost to nije točno jer se promet u priključnicama može presresti i nadzirati korištenjem tehnike koja se naziva ometanje protokola razlučivanja adresa[5] (eng. *Address Resolution Protocol - ARP*). Čak iako se ovaj problem može lako riješiti još uvijek postoje napadi na fizičke medije koji se vrlo lako izvode. Usmjeritelj (eng. *router*) najčešće pokreće neki program. Primjerice usmjeritelj tvrtke Cisco pokreće operacijski sustav iOS koji je napisan u programskom jeziku C te je moguće iskoristiti njegove ranjivosti. Napadi na razini mreže nisu teški za napraviti, a postoje i alati koji ih lako automatiziraju.

5.4. Smanjenje površine za napad

Za veliku aplikaciju, teška, ali pouzdana, metrika za određivanje ukupnog rizika je izmjeriti broj ulaznih točaka koje aplikacija ima te se to zove površina napada. Više ulaznih točaka u aplikaciju pruža više načina na koje napadač može pronaći slabosti. Naravno, bilo koja metrika mora uzeti

[5] Protokol razlučivanja adresa (eng. *Address Resolution Protocol - ARP*) je komunikacijski protokol kojim se dobiva fizička adresa na lokalnoj mreži iz poznate mrežne adrese. Najraširenija njegova primjena danas je na Ethernetu gdje se IP adrese povezuju s MAC (eng. *Media Access Control*) adresama

u obzir dostupnost ulazne točke. Primjerice, puno aplikacija napravljeno je za model prijetnji gdje se vjeruje lokalnoj okolini. U ovom slučaju veliki broj ulaznih lokalnih točaka (kao što su datoteke za konfiguraciju, *registry* ključevi, ulazi za korisnike i sl.) trebao bi manje zabrinjavati nego stvaranje nekoliko vanjskih mrežnih veza. Prebacivanje funkcionalnosti koje su se prije nalazile na nekoliko priključnica na jednu priključnicu uvijek pomaže smanjiti površinu za napad, osobito kad samostalna priključnica ima sve iste funkcionalnosti s infrastrukturom koja obavlja osnovno prebacivanje. Efektivna površina napada ostaje ista osim ako se stvarna funkcionalnost nekako ne pojednostavi. Budući da osnovna složenost utječe na mogućnost napada, metrika koja se zasniva na površini napada ne bi se trebala koristiti kao jedino sredstvo za provjeru pristupa nego bi trebala biti obvezna analiza rizika u dijelu programa.

5.5. Sigurnost sa zadanim postavkama

Zadane postavke sustava ne bi trebale izlagati korisnika nepotrebnim rizicima te bi trebale biti sigurnije što je to više moguće. Sve sigurnosne funkcionalnosti trebale bi u početku biti omogućene, dok bi dodatne mogućnosti koje uzrokuju bilo kakav rizik trebale biti onemogućene. Ukoliko postoji kvar u sustavu on ne bi smio uzrokovati nesigurnost koju napadači mogu iskoristiti. Ovaj način nije baš u potpunosti upotrebljiv, ali je korisnicima najjednostavnije koristiti sustav kada su sve funkcionalnosti odmah omogućene. Korisnici mogu koristiti mogućnosti koje su im potrebne i ignorirati one koje nisu. Međutim, napadači neće ignorirati te mogućnosti. Sustavi koji radi s nesigurnim zadanim postavkama konfiguracije su ranjivi. U mnogim slučajevima, može biti teško nadograditi sustav prije nego ga ugroze napadači. Stoga, ako postoje značajni sigurnosni rizici koje korisnici nisu prihvatili treba napraviti konfiguraciju koja ima zadane postavke sigurne . U sustavu u kojem su zadane postavke sigurne korisnik će trebati sam omogućiti funkcionalnosti koje povećavaju rizik.

5.6. Principi za smanjenje izloženosti sustava

U podmornicama postoji mogućnost izoliranja pojedinih komora što je čini sigurnijom za ljude koji se u njoj nalaze. Ako dođe do proboja trupa i u taj dio podmornice uđe voda, ljudi koji se nalaze u njoj će vjerojatno preživjeti zbog podjele podmornice na odvojene hermetičke komore. Ako se jedna komora napuni vodom ona se može izolirati od ostalih komora. Dijeljenje u komore je dobar princip prilikom izrade programskih sustava. Osnovna ideja je pokušati zadržati štetu ako nešto pođe po zlu. Neki principi za smanjenje izloženosti sustava su:

- princip s najmanjim povlasticama - navodi kako bi povlastice koje su dodijeljene korisniku trebale biti ograničene samo na one koje su mu potrebne. Na primjer, ovaj princip kaže kako korisnici ne bi trebali pokretati programe s privilegijama administratora ako je to moguće. Umjesto toga trebalo bi ih pokretati kao obični korisnik koji ima dovoljno privilegija za obavljanje tog posla.
- princip smanjenja prozora ranjivosti - kada rizik mora biti uveden, trebao bi biti prisutan što je kraće moguće. U kontekstu privilegija, trebalo bi odrediti koje privilegije korisnik može imati te mu ih omogućiti samo kada je to potrebno. Vrlo učinkovita tehnologija za provedbu ovih načela je pojam razdvajanja privilegija. Ideja je podijeliti aplikaciju u dva dijela, privilegiranu jezgru i glavnu primjenu. Privilegirana jezgra ima što je manje mogućnosti kako bi se mogla dobro provjeravati. Ova tehnika odjeljuje svakog korisnika u njegov vlastiti proces te u potpunosti uklanja pristup privilegijama, osim onima koje su potrebne. Zatim neizravno omogućuje neophodne privilegije samo na mjestu gdje su potrebne.

5.7. Princip nesigurnog pokretanja

Ako korisnik mora koristiti nesigurni komunikacijski kanal, trebao bi ga koristiti za pokretanje sigurnog komunikacijskog kanala. Primjerice protokol SSH (eng. *Secure Shell*) omogućuje sigurni kanal nakon što klijent i poslužitelj međusobno provjere autentičnost. Budući da ne koriste infrastrukturu s javnim ključem, prvi put kada se klijent spoji on neće imati podatke poslužitelja.

Poslužitelj šalje podatke za prijavu te ih klijent prihvaća u uvjerenju kako su oni ispravni. Ako neki napadač može poslati svoje podatke za prijavu tada se može maskirati kao poslužitelj ili pokrenuti napad. No, klijent koji koristi protokol SSH može zapamtiti podatke za prijavu. Ako ovi podaci ostanu isti, tada je i prvo povezivanje bilo sigurno te su kasnije veze isto sigurne. Ako se podaci za prijavu promijene, tada se može zaključiti kako postoji problem. Najbolje je ne koristiti nesigurne kanale ako se oni mogu zaobići.

5.8. Provjera valjanosti ulaza

Ako program prihvaća različite neprovjerene ulaze, često se pokušava otkriti kako će napadač pronaći ulaz koji ima negativne sigurnosne posljedice. Nekoliko velikih kategorija problema sigurnosti programa su:

- konačni problemi provjere valjanosti ulaza koji uključuju preljev međuspremnika,
- napadi umetanjem SQL koda (eng. *SQL injection attacks*) i
- napadi umetanjem naredbi (eng. *command-injection attacks*).

Unos podataka u program može biti valjan ili nevaljan, ovisno o semantici programa. Dobra sigurnosna praksa je konačno utvrditi sve neispravne podatke prije nego se poduzimaju bilo kakve radnje na podacima. Ukoliko su podaci neispravni treba poduzeti odgovarajuće radnje.

5.9. Defense in depth

Princip strategije Defense in depth je u tome što slojeviti sigurnosni mehanizmi povećavaju sigurnost sustava u cjelini. Ako zbog napada jedan sigurnosni mehanizam više ne radi ispravno, ostali mehanizmi i dalje mogu pružiti potrebnu sigurnost kako bi zaštitili sustav. Primjerice, nije dobra ideja potpuno se oslanjati na vatrozid i misliti kako će on omogućiti sigurnost za aplikacije koje se koriste izvan sustava. Vatrozid obično može zaobići uporni napadač (čak i ako je potreban fizički napad ili napad socijalnog inženjeringa). Ostali sigurnosni mehanizmi trebali bi se dodati kako bi upotpunili zaštitu koju pruža vatrozid. Primjena strategije Defense in depth može povećati složenost aplikacije i u suprotnosti je s načelom jednostavnosti koji se često koristi u sigurnosti. Neki bi mogli reći kako dodavanje novih mogućnosti za zaštitu donosi dodatnu složenost koja može donijeti nove rizike. Ukupni rizik sustava mora se dobro procijeniti. Na primjer, aplikacija koja za provjeru autentičnosti korisnika koristi korisničko ime i lozinku možda neće imati korist od povećanja duljine lozinke s 8 na 15 znakova. Povećana složenost natjerat će korisnike na zapisivanje lozinke te na taj način smanjiti ukupnu sigurnost sustava. No, dodavanjem pametne kartice [6](eng. *smart card*) za provjeru autentičnosti unaprijedit će sigurnost aplikacije jer se dodaje komplementaran sloj u procesu za provjeru autentičnosti.

5.10. Pozitivni sigurnosni model

Ovaj model je princip ili skup principa te je poznat pod nazivom „bijela lista“ (eng. *whitelist*). Pozitivni sigurnosni model (eng. *Positive security model*) definira što je dozvoljeno te odbacuje sve drugo. Trebao bi biti u kontrastu s „negativnim“ (ili „blacklist“) sigurnosnim modelom u koje se definira ono što nije dozvoljeno dok prešutno dopušta sve drugo. Pozitivni sigurnosni model može se primijeniti na veliki broj različitih područja primjene sigurnosti. Primjerice, prilikom obavljanja ulazne provjere valjanosti, ovaj model nalaže korisnicima kako bi trebali odrediti svojstva za ulazne parametre koji će biti dopušteni. To je suprotno pokušajima u kojima se pokušavaju filtrirati loši ulazi. U području provjere pristupa, pozitivni sigurnosni model svemu onemogućava pristup te dopušta pristup samo određenim ovlaštenim resursima ili funkcijama. Ovaj pristup može se pronaći u mrežnom vatrozidu. Prednosti korištenja pozitivnog sigurnosnog modela je u tome što će novi napadi, koje nije predvidio razvojni programer, biti spriječeni.

[6] Pametne kartice (eng. smart card) je malena plastična kartica s ugrađenim računalnim čipom. Pametna se kartica koristi zajedno s osobnim identifikacijskim brojevima (eng. *Personal Identification Number* - PIN) za prijavu na mrežu, računalo ili uređaj. Korištenje pametne kartice jača je mjera zaštite od lozinke jer je puno teže ukrasti pametnu karticu i saznati PIN nego saznati lozinku.

Međutim, negativni sigurnosni model može biti vrlo primamljiv kada se pokušavaju spriječiti napadi na web stranici. U konačnici, usvajanje negativnog sigurnosnog modela znači kako korisnici nikada neće moći biti u potpunosti sigurni jesu li sve napade stavili na popis. Korisnik će na kraju imati dugačak popis negativnih potpisa kojeg treba svakodnevno održavati i nadopunjavati.

5.11. Propust sigurnosti

Sigurno rješavanje pogreška ključni je aspekt sigurnosnog kodiranja. Postoje dvije vrste pogrešaka koje zaslužuju posebnu pažnju. Prva je iznimka koja se pojavljuje u obradi sigurnosne provjere. Vrlo je važno da ova iznimka ne omogući ponašanje koje se u normalnim okolnostima ne bi dopustilo. Razvojni programeri trebali bi uzeti u obzir kako uglavnom postoje tri moguća ishoda (prikazano na Slika 4) ovog sigurnosnog mehanizma:

- dopustiti operaciju,
- zabraniti operaciju,
- iznimka.

Slika 4. Prikaz tri moguća ishoda sigurnosnog mehanizma
Izvor: CIS

U principu, razvojni programeri trebali bi napraviti sigurnosni mehanizam kako bi neuspjeh pratio isti izvršni put kao i nedopuštanje izvođenja operacije. Primjerice, sigurnosne metode kao „je li ovašten“ („*isAuthorized()*“), „je li autoriziran“ („*isAuthenticated()*“) i „potvrdi“ („*validate()*“) trebale bi vraćati vrijednost „netočno“ ako postoji iznimka tijekom procesa. Ako sigurnosne provjere mogu dati iznimke, one moraju biti vrlo jasne o tome što takvo stanje znači. Druga vrsta važne sigurnosne iznimke je u kodu koji nije dio sigurnosne provjere. Ovakve iznimke su vrlo važne za sigurnost ako utječu na pravilno pozivanje kontrola. Iznimka može izazvati da se sigurnosna metoda ne poziva kada bi trebala ili može utjecati na inicijalizaciju varijabli koje se koriste u sigurnosnoj provjeri.

5.12. Najmanja privilegija

Princip najmanje privilegije (eng. *Least privilege*) preporuča dodjelu najmanje količine privilegija koje su potrebne za obavljanje poslovnih procesa korisničkim računima. To obuhvaća korisnička prava, dozvole za resurse kao što su ograničenja središnje procesirajuće jedinice[7] (eng. *Central Processing Unit* - CPU) , memoriju, mrežu i dozvole sustava datoteka. Primjer je ako poslužitelj zahtjeva samo pristup mreži, mogućnost čitanja baze podataka i mogućnost pisanja u zapisnik te to opisuje sva dopuštenja koja bi trebala biti odobrena. Ni pod kojim uvjetima poslužitelj ne bi smio imati administrativne privilegije.

[7] Središnja procesirajuća jedinica (eng. *Central Processing Unit* - CPU) je središnji dio računala koji vođen zadanim programskim naredbama izvodi osnovne radnje nad podacima. Procesor također tipično upravlja i svim ostalim dijelovima računala. Kako su današnji procesori slični u nekim tehnološkim značajkama, obično se dijele prema brzini rada, veličini podatka nad kojim mogu odjednom obaviti zadanu radnju te prema karakteristikama unutarnjeg ustroja.

5.13. Izbjegavanje sigurnosti s nepoznatim

Sigurnost putem nepoznatog je oslanjanje na tajnost primjene sustava ili komponenti sustava kako bi održali sustav sigurnim. Izbjegavanje sigurnosti s nepoznatim (eng. *Security though obscurity*) slaba je sigurnosna provjera koja skoro uvijek iznevjeri korisnike kada se koristi samo ona za provjeru. To ne znači kako je čuvanje tajni loša ideja, nego kako se izrada ili logika sigurnosne provjere treba zasnivati na otvorenim i poznatim principima. Primjerice, u kriptografskim sustavima, potreban je samo ključ kako bi se zadržala tajna, odnosno ne treba se oslanjati na čuvanje algoritama kao tajne kako bi sustavi ostali sigurni.

5.14. Jednostavnost

Površina napada i jednostavnost idu zajedno. Razvojni programeri trebali bi izbjegavati korištenje dvostrukih negativa i složenih arhitektura u slučajevima kada bi jednostavniji pristup bio brži i jednostavniji.

5.15. Otkrivanje provala

Otkrivanje provala u sustav zahtjeva tri elementa:

- sposobnost zapisivanja događaja koji su važni za sigurnost,
- postupci koji osiguravaju regularno nadziranje zapisnika,
- postupci za ispravno odgovaranja na upade u sustava jednom kada se otkriju.

Korisnici bi trebali zapisivati sve informacije koje su važne za sigurnost sustava. Možda se tada uspije otkriti problem pregledavanjem tih zapisa koji se nije uspio otkriti za vrijeme izvođenja, no potrebno je zapisati dovoljno informacija. Svako korištenje sigurnosnih mehanizama treba se zapisati s dovoljno informacija kako bi se mogao pratiti i pronaći počinitelj. Osim toga zapisivanjem funkcionalnosti u aplikaciju trebalo bi pružiti metodu za upravljanje zapisanim informacijama. Ako sigurnosni analitičar nije u mogućnosti analizirati zapise događaja kako bi odredio koji od događaja su djelotvorni, tada zapisane informacije imaju vrlo malu vrijednost. Otkrivanje upada u sustav važno je jer se u suprotnom slučaju daje napadaču neograničeno vrijeme za usavršavanje svog napada. Ako je otkriven upad u sustav, tada će napadač imati samo jedan pokušaj prije nego se otkrije i spriječi daljnji pokušaji napada. Ukoliko korisnik primi zahtjev kojeg zakoniti korisnik nije mogao napraviti to je onda napad te je potrebno u skladu s tim reagirati. Zapisivanje informacija omogućuje forenzičku funkciju za aplikaciju ili web stranicu. Ako je aplikacija ili web stranica napadnuta, može se pratiti krivac te provjeriti što je bilo krivo. Ukoliko korisnik koristi anonimni (eng. *anonymizing*) posrednik, dobri zapisi će pomoći otkriti što se dogodilo te se ranjivost može brže i lakše popraviti. Ne treba se oslanjati na druge tehnologije za otkrivanje upada u sustav. Kod korisnika je jedina komponenta sustava koja ima dovoljno informacija za otkrivanje napada. Nitko drugo neće znati koji parametri su točni, koje radnje su omogućene korisniku na odabir i slično.

5.16. Ne treba vjerovati uslugama

Usluge se mogu odnositi na bilo koji vanjski sustav. Mnoge organizacije koriste procesorske mogućnosti od drugih partnera koji vjerojatno imaju različita sigurnosna pravila i stavove. Malo je vjerojatno kako korisnik može utjecati ili provjeravati vanjske korisnike, bilo da su oni kućni korisnici, veliki dobavljači ili partneri. Prema tome, vanjski sustavi trebali bi biti provjeravani te im ne treba vjerovati. Primjerice, pružatelj programa povjerenja daje podatke koji se koriste za Internet bankarstvo te pruža nekoliko nagradnih bodova i mali popis mogućih predmeta koji se mogu s njima otkupiti. Međutim, podaci bi se trebali provjeriti kako bi osigurali da je sigurno prikazati ih krajnjim korisnicima te kako su nagradni bodovi pozitivan broj.

5.17. Uspostava sigurnih zadanih postavki

Postoji puno načina za predstavljanje nesvakidašnjeg iskustva korisnicima. Međutim, iskustvo bi trebalo biti sigurno te bi korisnici sami trebali odlučiti ako žele smanjiti svoju sigurnost. Primjerice kao zadane postavke lozinke treba biti omogućena složenost. Korisnicima bi se moglo omogućiti gašenje ovih dviju mogućnosti kako bi pojednostavili korištenje svoje aplikacije i povećali rizik [3] i [4].

6. Zaključak

Strategija Defense in depth ima puno potencija za daljnji razvoj jer još uvijek nisu iskorištene sve njezine mogućnosti. Pretvaranjem ove strategije iz stvarnog svijeta u računalni svijet došlo je do određenih pogrešaka jer ne vladaju isti zakoni. U stvarnom svijetu vladaju fizikalni zakoni kao što su stvarna udaljenost napadača od cilja i čvrste prepreke koje se ne mogu lako zaobići. U virtualnom, odnosno računalnom svijetu nije bitno nalazi li se neprijatelj do svog cilja ili se nalazi na drugom kraju svijeta. Napadači iskorištavaju nedostatke ove strategije pa bi ih u budućnosti trebalo popraviti. Vrlo pozitivna stvar strategije Defense in depth je što ima puno slojeva obrane te ako napad iskoristi ranjivosti jednog sloja ili uspije zaobići sigurnosne sustave na tom sloju, preostaju ostali slojevi koji mogu spriječiti napad. Jedan od razloga zašto strategija Defense in depth nije u potpunosti učinkovita je što ne može napasti svoje neprijatelje. U stvarnom svijetu prilikom borbe napadaju i neprijatelji i branitelji, dok u računalnom svijetu napada neprijatelj, a branitelj mu ne smije uzvratiti jer to nije zakonito u mnogim zemljama. Postoji još puno sigurnosnih principa koji se mogu koristiti za održavanje sigurnosti sustava i aplikacija. Korisnik prilikom izrade vlastitog sustava za sigurnost treba vidjeti što je njemu najvažnije te tako postaviti komponente strategije Defense in depth.

7. Leksikon pojmova

NIST (Institucija koja se bavi standardizacijom tehnologije)

Institucija koja se bavi standardizacijom tahnologije - Nekada poznata pod imenom NBS (National Bureau of Standards), NIST je agencija koja se bavi mjeriteljstvom, standardim i tehnologijama u cilju poboljšanja ekonomske sigurnosti i kvalitete života. - Nekada poznata pod imenom NBS (National Bureau of Standards), NIST je agencija koja se bavi mjeriteljstvom, standardizacijom tehnologija u cilju poboljšanja ekonomske sigurnosti i kvalitete života. http://www.nist.gov/public_affairs/overview_video/overview_video.html

DOS napad (Napad uskraćivanjem usluge)

Nekada poznata pod imenom NBS (National Bureau of Standards), NIST je agencija koja se bavi mjeriteljstvom, standardima i tehnologijama u cilju poboljšanja ekonomske sigurnosti i kvalitete života.

http://en.wikipedia.org/wiki/Denial-of-service_attack

Kriptologija (Znanost o kriptiranju i dekriptiranju)

Znanost koja obuhvaća pojmove kritpografije i kriptoanalize. Kriptografija je umješnost izmišljanja šifri, dok je kriptoanaliza umješnost njihova probijanja. http://searchsecurity.techtarget.com/definition/cryptology

Priključnica (Krajnje točke u komunikaciji transportnih protokola)

Brojčane vrijednosti temeljem kojih računalo po prihvatu podataka zna koju uslužnu programsku potporu (servise) mora aktivirati te na koji način razmjenjivati podatke na transportnom sloju. http://searchnetworking.techtarget.com/definition/port-number

TCP (Transmission Control Protocol)

Jedan od dva protokola usmjeravanja koja se koriste u Internetu, uspostavlja logičku vezu između krajnjih računala i osigurava pouzdani prijenos. TCP se nalazi na transportnom sloju OSI modela. - Jedan od dva protokola usmjeravanja koja se koriste u Internetu. Uspostavlja logičku vezu između krajnjih računala i osigurava pouzdani prijenos. http://www.webopedia.com/TERM/T/TCP.html

IP (IP protokol - Internet Protocol)

IP je jedan od glavnih protokola u Internetu, a koristi se za usmjeravanja paketa kroz Internet. U tu namjenu, dodjeljuje IP adrese izvora paketa i njegovog odredišta na temelju kojih će se paketi usmjeravati kroz nekoliko računalnih mreža. http://compnetworking.about.com/od/networkprotocolsip/g/ip_protocol.htm

Autentikacija (Autentikacija je proces potvrđivanja identiteta podatka ili osobe)

Autentikacija je proces određivanja identiteta nekog subjekta, najčešće se odnosi na fizičku osobu. U praksi subjekt daje određene podatke po kojima druga strana može utvrditi da je subjekt upravo taj kojim se predstavlja. Najčešći primjeri su: uz korištenje kartice na bankomatu i upisivanje PIN-a, ili upisivanje (korisničkog) imena i zaporke. http://searchsecurity.techtarget.com/definition/authentication

Virus (Računalni virus)

Virusi su programi koji se mogu kopirati i zaraziti računalo bez znanja ili dopuštenja korisnika. Računalo se može zaraziti na razne načine preko Internet-a, CD-a, USB-a... Virusi dolaze većinom sa drugim programima, kao što su npr. Trojanski konji kako bi maskirali svoj rad i kako bi ih bilo još teže za otkriti. Namjene virusa su različite, mogu služiti samo kako bi radili štetu no neki su manje štetni i samo usporavaju računalo i smetaju korisniku u radu. Virusi se spremaju u memoriju računala

i pokreću se s operacijskim sustavom i inficiraju programe koji se pokreću. http://www.ust.hk/itsc/antivirus/general/whatis.html

Sigurnosna stijena (Firewall)

Sigurnosna stijena (engl. Firewall) je skup komunikacijskih nakupina koji služe kako bi odvojili privatnu mrežu od javne. Sastoje se od programa koji služe kako bi pratili i upravljali promet između računala i mreža. Sigurnosne stijene mogu propuštati, blokirati, šifrirati promet na temelju pravila koja korisnik postavlja. http://searchsecurity.techtarget.com/definition/firewall

Trojanski konj (Zloćudni program koji se pretvara kao legitimna aplikacija)

Trojanski konj je oblik zloćudnog programa koji se pretvara kao legitimna aplikacija. U početku se pretvara kao da obavlja korisnu funkcionalnost za korisnika, no u pozadini izvodi štetne radnje (na primjer, krađa informacija). Za razliku od crva, ovaj oblik zloćudnih programa se ne širi samostalno. http://www.webopedia.com/TERM/T/Trojan_horse.html

Certification Authority (Tijelo za izdavanje digitalnih certifikata)

U kriptografiji, izdavatelj certifikata (eng. Certification Authority, CA) je osoba koja izdaje digitalne certifikate. U modelu povjerenja, CA je pouzdajuća treća strana kojoj vjeruje vlasnik certifikata i stranka koja se oslanja na certifikat. CA je karakteristika mnogih shema infrastrukture javnih ključeva (eng. Public key infrastructure, PKI). http://searchsecurity.techtarget.com/definition/certificate-authority

Kriptografija (Kriptografija u računarstvu)

Kriptografija je područje kriptologije koje se bavi stvaranjem kriptografskih algoritama za zaštitu podataka. Točnije, podrazumijeva stvaranje i analizu protokola i algoritama koji osiguravaju siguran prijenos i pohranu informacija, bilo u računalnoj mreži ili mediju za pohranu podataka.

http://searchsoftwarequality.techtarget.com/definition/cryptography

Cyber kriminalac (Osoba koja se bavi cyber kriminalom)

Cyber kriminalac je osoba koja koristi računala i Internet za počinjenje kaznenih dijela. http://www.webopedia.com/TERM/C/cyber_crime.html

Usmjeritelj (Uređaj koji usmjerava pakete između računalnih mreža)

Usmjeritelji su uređaji koji imaju barem dva sučelja na različitim mrežama, a usmjeravaju pakete do njihovog odredišta. Na svom putu, paketi prolaze kroz nekoliko usmjeritelja, a svaki zasebno određuje put kojim će ga dalje slati.

http://www.webopedia.com/TERM/R/router.html

9. Reference

[1] Prescott E. Small: Defense in Depth: An Impractical Strategy for a Cyber World, http://www.sans.org/reading_room/whitepapers/assurance/Defense-depth-impractical-strategy-cyber-world_33896, studeni 2011.

[2] Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments, http://www.nsa.gov/ia/_files/support/Defenseindepth.pdf, lipanj 2012.

[3] OWASP: The Open Web Application Security Project: Category:Principle, https://www.owasp.org/index.php/Category:Principle, lipanj 2012.

[4] OWASP: The Open Web Application Security Project: CLASP Security Principles, https://www.owasp.org/index.php/CLASP_Security_Principles, lipanj 2012.

[5] Victor Hazlewood: Defense-In-Depth: An Information Assurance Strategy for the Enterprise, http://www.sdsc.edu/~victor/DefenseInDepthWhitePaper.pdf, 2006.

[6] Wikipedia: Defence in depth, http://en.wikipedia.org/wiki/Defence_in_depth, lipanj 2012.

[7] Wikipedia: Defense in depth (computing), http://en.wikipedia.org/wiki/Defense_in_depth_(computing), lipanj 2012.

[8] The Antivirus Defense-in-Depth Guide, http://academy.delmar.edu/Courses/ITNW1454/Handouts/AntivirusDefenseInDepth-Chapter3_AntivirusDefense-in-Depth.htm, svibanj 2004.