VODIČ:

BEZBEDNOST ORGANIZACIJA U DIGITALNOM OKRUŽENJU

KAKO SAČUVATI PRIVATNOST I POVERLJIVOST DIGITALNE KOMUNIKACIJE

Priručnik za pametno upravljanje informacionim sistemima medijskih i građanskih organizacija: osnove čuvanja, obrade i razmene podataka

SHARE FOUNDATION - 2015

vodič

"BEZBEDNOST ORGANIZACIJA U DIGITALNOM OKRUŽENJU"
SHARE FONDACIJA
OKTOBAR 2015
UREDNICI: ĐORĐE KRIVOKAPIĆ, VLADAN JOLER
TEKSTOVI: ANDREJ PETROVSKI
LEKTURA: MILICA JOVANOVIĆ
DIZAJN I PRELOM: OLIVIA SOLIS VILLAVERDE

ŠTAMPARIJA: NS PRESS DOO NOVI SAD
TIRAŽ : 200

PODRŠKA PROJEKTU:

CIVIL RIGHTS DEFENDERS

CIP - Каталогизација у публикацији
Библиотека Матице српске, Нови Сад
316.774:004.738.5.056(036)
ПЕТРОВСКИ, Андреј
Bezbednost organizacija u digitalnom okruženju : vodič : kako sačuvati privatnost i poverljivost digitalne komunikacije / [tekstovi Andrej Petrovski, Katarina Ercegović]. - Novi Sad : Share foundation, 2015 (Novi Sad : NS press). - 28 str. : ilustr. ; 16 cm
Tiraž 200.
ISBN 978-86-89487-04-6
1. Ерцеговић, Катарина [аутор]
a) Медијске куће - Интернет - Безбедност - Водичи
COBISS.SR-ID 302299399

UVOD

Novinarski posao i građansko organizovanje u zajednici - od kojih se očekuje blagovremeno i tačno informisanje javnosti i zaštita javnog interesa - u digitalnoj eri nisu mogući bez odgovarajuće tehničke zaštite osetljivih podataka. Od internog poslovanja, organizacionih planova i komunikacije sa poverljivim izvorima sve do objavljenog sadržaja na internetu, čitav informacioni sistem medija i organizacija civilnog društva sačinjen je od podataka čiji je integritet neophodno sačuvati. Na prvoj liniji fronta u borbi za javni interes, novinarima i aktivistima na mreži pridružili su se administratori i vebmasteri.

Ovaj vodič je namenjen upravo tehničkoj posadi informacionih sistema u medijskim i građanskim organizacijama, koji imaju potrebu da uobičajena znanja o hardveru i softveru dopune lekcijama o njihovoj zaštiti.

Nema univerzalnog rešenja za tehničku bezbednost organizacija, ne samo usled činjenice da se novi alati i strategije za napad razvijaju gotovo svakodnevno. Pojedine organizacije imaju različite potrebe koje tehnički administratori dobro poznaju i kojima će lako prilagoditi opšti pregled zaštite ključnih tačaka sistema iz ovog vodiča.

SHARE Fondacija aktivno sarađuje sa novinarima, aktivistima, medijskim i građanskim organizacijama u borbi protiv sajber napada i pruža im tehničku i pravnu pomoć. Iz tog iskustva formirana je baza znanja i preporuka, objavljenih u seriji vodiča o različitim aspektima tehničke i pravne zaštite medija.

Nakon priručnika "Osnove digitalne bezbednosti", namenjenog individualnoj zaštiti novinara i medijskih radnika, ovaj vodič preduzima sledeći logičan korak - kako omogućiti sistemsku bezbednost na nivou medijske organizacije.

INFO BOX:

- Informaciona privatnost se odnosi na čuvanje, reprodukciju, razmenu i prikazivanje informacija i metapodataka o ličnosti ili organizaciji.
- Digitalna bezbednost je zaštita onlajn naloga, računara, datoteka i sistema od napada.

ULAZ U SISTEM

DOBRA LOZINKA

Ponekad se usled prilično zahtevnog uspostavljanja složenog sistema dešava da se previdi pitanje lozinke, elementarnog nivoa zaštite. Kao najčešće korišćen metod odobravanja pristupa, lozinke treba da budu što kompleksnije. Za početak, treba savladati naviku da se za kriterijum dobre šifre uzima koliko se lako pamti.

Osnovno pravilo pri kreiranju šifre jeste izbegavanje podataka iz privatnog života - datum rođe-nja, ime kućnog ljubimca, omiljeno mesto i slično - kao i bilo reči prirodnog jezika. Klasične metode probijanja lozinke danas podrazumevaju automatizovane pretrage po spiskovima reči (Dictionary attack) koji mogu obuhvatiti na milione pojmova iz različitih jezika.

Šifra od 12 brojeva ili manje, može se razbiti za manje od sat vremena. Sa tehnologijom u slobodnoj prodaji, potrebno je oko pet miliona godina da bi se probila šifra iste dužine koja, osim brojeva, sadrži velika i mala slova i specijalne karaktere.

INFO BOX:

Šifra od 12 brojeva ima 1.000.000.000.000 kombinacija, preciznije 10^{12}, Šifra od 12 znakova koja sadrži cifre, velika i mala slova i specijalne karaktere ima 475.920.310.000.000.000.000.000 kombinacija, imajući u vidu da je ukupan broj svih alfanumeričkih i specijalnih karaktera 94.

TOP LISTA PROBIJENIH LOZINKI U 2014.

- 123456
- password
- 12345
- 12345678
- qwerty

PRIMERI DOBRE LOZINKE
(objavljene ovde postaju neupotrebljive)

- uTD3Kyax7s8B+u6N
- @^635JusAWtpGxH
- #q@Bd3z4+Lq3W _ gh
- -xA-GCecLe3Nq2bA
- yrPb9R2Hw9^S8Qnv

Nažalost, kvalitetnu šifru teško je zapamtiti. Trebalo bi iskoreni- ti još jednu lošu naviku - zapisivanje šifre na papir ili čuvanje na telefonu. Lozinke su najsigurnije kada se kriptuju i pohrane u bazu podataka, gde ostaju nedostupne čak i u slučaju da je računar na kom se šifre čuvaju meta napada. Primer takve aplikacije je KeePass;

http://keepass.info/

INTERNA MREŽA

U redakciji su svi računari, štampači, uređaji za skladištenje (storage servers ili mini data centres), mejl serveri, ruteri i ostale komponente povezani u internu, lokalnu mrežu, fizički (kablom) ili bežično (wi-fi).

Ove mreže su najčešće bazirane na takozvanoj klijent - server arhitekturi. Klijent ili korisnik je računar ili neka druga hardverska komponenta u svakodnevnoj upotrebi, dok je server poseban računar koji klijentima omogućava korišćenje resursa koji se na njemu čuvaju. To mogu biti sadržaji poput aplikacija, veb strana, datoteka, imejl poruka, baza podataka itd. Postoje različite vrste servera, web server, file server, mail server, database server itd.

S obzirom na to da je koncentracija osetljivih podataka u ovoj mreži velika, na nju se primenjuju posebne mere zaštite.

BEŽIČNA MREŽA

Bežična mreža može da ima različiti fizički opseg u zavisnosti od jačine emitovanog signala. U zatvorenoj prostoriji taj opseg prosečno iznosi dvadesetak metara oko rutera, što često znači da je ova mreža dostupna i izvan redakcije.

Ruteri koji emituju bežični signal imaju nekoliko slojeva zaštite, čija je konfiguracija zadatak administratora.

NAJČEŠĆE MERE ZAŠTITE:

- **WIRELESS SECURITY MODE:** Preporučuje se korišćenje WPA2 (Wifi Protected Access 2) zaštite koja ima dve moguće primene. PSK (Pre-Shared-Key) se podešava jednostavno, postavljanjem šifre; Enterprise zahteva nešto komplikovanije podešavanje i dodatni RADIUS (Remote Authentication Dial In User Server) server.

U većini slučajeva, PSK metod je dovoljno dobar mehanizam zaštite za male i srednje organizacije, ukoliko postavljena šifra zadovoljava standarde. Veliki broj rutera podržava i WPS (Wi-Fi Protected Setup), sistem koji omogućava logovanje na bežičnu mrežu pomoću dugmeta na ruteru, bez unošenja šifre. Ovaj sistem ima ozbiljne bezbednosne nedostatke, pa se preporučuje da na ruteru bude isključen.

Sigurnosni protokoli koji su se ranije koristili (WEP i WPA) napušteni su zbog bezbednosnih nedostataka.

- **MAC FILTRIRANJE:** MAC adresa je fizička adresa uređaja koji se povezuje na mrežu. Ruter može da se podesi tako da omogući pristup samo adresama koje se nalaze na njegovoj listi. Ovaj metod neće zaustaviti napredne napadače, koji uz pomoć softvera kao što je Aircrack-ng mogu da otkriju listu MAC adresa sa rutera i neku od povezanih adresa preuzmu za svoj uređaj.
- **SAKRIVANJE SSID-A (SERVICE SET IDENTIFIER):** SSID je naziv mreže koji je obično javan. Slično kao i MAC filter, sakrivanje SSID-a neće zaustaviti napredne krakere, ali će sprečiti neke manje sposobne napadače da se igraju s tuđom mrežom.

Korišćenje više bežičnih mreža se preporučuje kada postoje najmanje dve kategorije ljudi kojima bi mreža bila namenjena, na primer zaposleni i gosti. S obzirom na karakteristike bežične mreže, jedini način da se mreža koju koriste zaposleni fizički odvoji od mreže na koju se povezuju ostali posetioci redakcije, jeste održavanje zasebnih rutera gde će svako imati svoj kabl koji ga povezuje direktno sa internet provajderom.

MERE FIZIČKE ZAŠTITE:
IZVAN MREŽE (AIR GAPPING)

Air gapping je mera zaštite u kojoj se pojedini računari ili grupa međusobno umreženih računara drže u izolaciji, odnosno ne povezuju se ni direktno ni posredno na javni Internet. Air gapping se primenjuje na delove sistema koji skladište ili obrađuju osetljive podatke. Ova bezbednosna mera je jedna od najefikasnijih metoda za sprečavanje upada u mrežu i krađe podataka.

Uz air gapping, na raspolaganju su i druge mere fizičke zaštite mreže, kao što je sprečavanje upotrebe USB ulaza. Jedan od najsloženijih kompjuterskih virusa, Stuxnet, prenosi se najčešće preko USB fleš diska, kako su i zaraženi kontrolni sistemi nuklearnih postrojenja u Iranu 2010. iako nisu bili povezani na Internet.

DATA CENTAR

Decentralizacija sistema postavlja se kao ključni uslov njegove bezbednosti. Preporučuje se da se podaci ne čuvaju na istom računaru sa kog se unose u mrežu ili na kom se obrađuju. Računari koji imaju više namena podložniji su kvarovima, dok potencijalni napad može imati znatno veće posledice po sistem nego u slučaju da su računari ili serveri odvojeni jedni od drugih.

Postoji više načina za čuvanje velikih količina podataka. Najjednostavnije je skladištenje podataka na eksternom hard disku. Eksterni hard diskovi sa relativno dobrim performansama imaju pristupačne cene, ali ova vrsta kompjuterskog hardvera nema ugrađen mehanizam dupliranja (redundantnosti). To znači da bi u slučaju kvara (što i nije tako retka pojava) veći deo podataka koji su se nalazili na tom disku bio zauvek izgubljen. Sa druge strane, eksterni diskovi nemaju direktan izlaz na Internet i aktivni su jedino kad su povezani sa računarom, pa se može reći da su relativno bezbedni. Čuvanje podataka na eksternom hard disku znači da podaci ostaju u fizičkom sedištu organizacije.

Iz perspektive rizika od gubitka

podataka, iznajmljivanje prostora za čuvanje podataka na nekom cloud serveru znatno je bolji način za čuvanje važnih podataka. Cloud usluge koriste RAID tehnologiju što značajno smanjuje rizik u slučaju kvara. RAID (Redundant Array of Independent Disks) je tehnologija zasnovana na modelu uporednog korišćenja više diskova za skladištenje podataka, pri čemu se svaki podatak nalazi na najmanje dve lokacije. Međutim, ukoliko se radi o osetljivim podacima, ne preporučuje se čuvanje na tuđim uređajima i pored toga što svi cloud servisi uključuju kriptovanje.

Treći način skladištenja podataka jeste formiranje sopstvenog mini data centra u kome će se čuvati svi podaci od značaja za organizaciju. Oprema za ovu namenu zavisi od potreba. U ponudi se može naći niz gotovih rešenja koja su jeftinija i mogu trajno rešiti ovo pitanje. Tako će podaci ostati u okviru fizičkog prostora organizacije, a primenom RAID tehnologije smanjiće se rizik od gubitka i krađe podataka.

CLOUD STORAGE REŠENJA:

- Google Drive (https://drive.google.com/)
- DropBox (https://www.dropbox.com/)
- OneDrive (https://onedrive.live.com/)
- SpiderOak (https://spideroak.com/)
- Wuala (http://wuala.com/)
- Tresorit (https://tresorit.com/)

GOTOVA DATA CENTAR REŠENJA:

- Drobo (http://www.drobo.com/)

INFO BOX:

CLOUD COMPUTING je Internet tehnologija zasnovana na daljinskom korišćenju resursa (protok podataka, prostor za skladištenje, radna memorija itd.) i njihove razmene između više aplikacija i korisnika. Cloud može biti privatni, javni ili hibridan.

REZERVNA KOPIJA (BACKUP)

Stvaranje rezervne kopije ne utiče na stepen bezbednosti samog sistema, ali je backup od ključnog značaja kada se posle bezbednosne krize javi potreba da se izgubljeni podaci povrate. Ponekad je na osnovu rezervne kopije moguće utvrditi uzrok pada sistema, rekonstrukcijom sigurnosnih propusta ili grešaka u sistemu, i slično.

Preporučuje se korišćenje backup sistema otvorenog koda, kao što je UrBackup (http://www.urbackup.org/). Prilikom odabira, treba voditi računa o tome da sistem za rezervne kopije pruža mogućnost brzog i preciznog povratka podataka, te da bude optimalan odnosno da ne opterećuje previše serverske ili resurse za skladištenje.

KRIPTOVANJE DISKOVA

Uz pomoć lozinke ili digitalnog sertifikata neovlašćenim licima se onemogućava čitanje sadržaja sa diska. Moguće je podesiti i dodatne parametre kao što su dvostepena autentifikacija, ključ za dekripciju ili provera autentičnosti na osnovu biometrijskih podataka. U većini slučajeva, kriptovanje štiti podatke i u slučaju krađe kompjutera ili hard diska.

SOFTVER ZA KRIPTOVANJE:

- **VERACRYPT** je modifikovana verzija ranije popularnog programa TrueCrypt čiji je razvoj prekinut i više ne prati bezbednosne standarde. VeraCrypt je program koji kriptuje podatke lokalno i dostupan je na sledećoj adresi: https://veracrypt.codeplex.com/
- **BOXCRYPTOR** je softver koji se uglavnom koristi za kriptovanje podataka na cloud-u. Dostupan je na sledećoj adresi: https://www.boxcryptor.com/en/download
- **BITLOCKER** je program za kriptovanje diskova na Microsoft Windows operativnim sistemima. Uputstvo za korišćenje BitLocker-a je dostupno na sledećoj adresi:
- http://windows.microsoft.com/en-us/windows/protect-files-bitlocker-drive-encryption
- **FILEVAULT** je program za kriptovanje diskova na Mac OSX platformama. Uputstvo za korišćenje se može naći na sledećoj adresi: https://support.apple.com/en-us/HT204837

RAD NA DALJINU

Pristup aplikacijama i podacima koji se fizički nalaze u redakciji moguć je, uz odgovarajuće dozvole, sa bilo kog kompjutera u svetu. Rad se novinarima i urednicima na ovaj način znatno olakšava, skraćuje vreme potrebno za obradu podataka i omogućava učešće u procesu rada sa terena.

Sa bezbednosnog stanovišta, rad na daljinu ima ozbiljne mane. Uspostavljanjem veze između mreže ili servera u redakciji i spoljašnjeg računara, otvara se mogućnost za MitM (Man in the Middle) napade. MitM je vrsta tehničkog napada u kom klijent i server nisu nužno izloženi opasnosti, ali napadač koristi nedostatke veze kako bi pristupio njihovoj komunikaciji i izvršio krađu podataka.

Bezbedan način za rad na daljinu je povezivanje putem VPN-a (Virtual Private Network - virtuelna privatna mreža). Reč je o usluzi stvaranja izdvojenog tunela između dva računara na javnoj mreži, koji se posebno kodira radi zaštite. Od više vrsta virtualnih privatnih mreža najsigurnije je koristiti tzv. protokol bezbednog prenosa podataka (TSL Transport Layer Security).

SHARE Fondacija uz pomoć partnera IPredator **https://ipredator.se/** pruža organizacijama usluge uspostavljanja i primene VPN sistema.

Jedan od najboljih softvera za primenu VPN-a na nivou organizacije je OpenVPN, dostupan na sledećoj adresi: **https://openvpn.net/index.php/access-server/pricing.html.**

PRIVATNI MEJL SERVER

Elektronska pošta predstavlja posebno osetljiv skup podataka u svakoj redakciji. Radi zaštite, svaka organizacija bi trebalo da obezbedi poseban namenski server za e-poštu (dedicated server). Na taj način se štiti od napada, dok se istovremeno ne prepušta jurisdikciji drugih država.

Osim samog sadržaja elektronske pošte, značaj podataka iz svakodnevne komunikacije čine takozvani metapodaci - informacije koje prilikom razmene mejlova generišu i razmenjuju softver i uređaji koji se koriste za slanje i primanje. Napadačima su metapodaci često važniji od sadržaja samog pisma,

jer oni nose precizne informacije o digitalnom kontekstu komunikacije.

Metapodaci se čuvaju na mejl serveru pa je i njegova zaštita specifična. Osnovni korak u tom smeru je blokiranje svih protokola (na primer, FTP ili HTTP) koji serveru nisu potrebni za obavljanje njegove primarne funkcije, tj. primanje i slanje elektronske pošte.

Namenski server se može iznajmiti u sklopu hosting paketa ili drugih usluga, ili organizacija može kupiti server sa posebnim softverom. Primer takvog softvera je iRedMail, dostupan na sledećoj adresi:

http://www.iredmail.org/.

OPŠTE PREPORUKE O ZAŠTITI INFRASTRUKTURE:

- Ruteri se mogu podesiti tako da odbijaju automatizovano prikupljanje informacija o sistemu preko tzv. footprinting metoda. Ovaj metod podrazumeva stvaranje skice mreže na osnovu otisaka koji se generišu slanjem digitalnih signala. Takođe treba obratiti pažnju da se usmeravanje podataka odvija po različitim protokolima, jer upravo oni mogu predstavljati glavni izvor informacija za napadače. Mapiranje trasa kojima se podaci prenose (tracerouting), detektovanje aktivnih uređaja na mreži (ping) i slične metode mogu napadaču otkriti čitavu infrastrukturu, odnosno broj i vrstu rutera, računara i način na koji su povezani. Pozitivna praksa nalaže da se ICMP zahtevi omoguće za veb server, dok se konfiguracija za ostale servere i internu mrežu podešava tako da se ovi zahtevi odbijaju.
- Nepotrebne serverske protokole bi takođe trebalo onemogućiti. Tako se, na primer, na mejl serveru može blokirati sve osim protokola koji se koriste za elektronsku poštu (IMAP, POP i sl.), dok se veb serveri mogu strukturno konfigurisati tako da se pristup omogućava samo javnim resursima. Pristup ostalim folderima i datotekama, kao i administratorskom delu portala treba da bude onemogućen da bi se izbegao neovlašćeni pristup i curenje podataka.
- Zatvoriti nepotrebne portove koje nijedna aplikacija na serveru ne koristi, odgovarajućom konfiguracijom mrežnih barijera (Firewall).
- Upotrebom sistema za detekciju upada identifikuje se i odbija sumnjivi saobraćaj i registruju se pokušaji footprinting-a.
- Korišćenjem anonimnih registracionih servisa mogu se sakriti podaci o registratoru domena, koji uz izvesnu nadoknadu krije identitet osobe odgovorne za određeni sajt.

Ipak, treba imati u vidu da se reputacija kredibilnog medija gradi kroz transparentnost, te se ova tehnika ne preporučuje u svakoj situaciji. Takođe, značajno je napomenuti da državni organi ili advokati u pojedinim slučajevima mogu podneti zahtev registru domena i dobiti ove podatke.

(https://www.godaddy.com/domain-addon/private-registration.aspx)

INFO BOX

- **SERVERSKI PORT** je ulazno/izlazna tačka na serveru koju aplikacije koriste za razmenu podataka. Port je logički koncept koji omogućava kanalisanje protoka podataka, što znači da svaka aplikacija koristi svoj port čime se pravi logička podela paketa.
- **SISTEM ZA DETEKCIJU UPADA** (Intrusion Detection System - IDS) je svaki softver ili hardver koji detektuje upade. Takvi sistemi su firewall, honneypot i mreže koje koriste Demilitarised Zone, Bastion arhitekture i slično.
- **FOOTPRINTING** je tehnika prikupljanja podataka o određenom IS pomoću različitih tehničkih alata, a cilj je između ostalog da se utvrdi struktura interne mreže, broj i vrsta uređaja na toj mreži, vrste operativnih sistema i drugih aplikacija na tim uređajima, informacije o portovima, i drugi podaci koji se mogu prikupiti neposrednom upotrebom tehnologije.

IZLAZ

ZAŠTITA KOMUNIKACIJE

ELEKTRONSKA POŠTA

Korišćenjem namenskog mejl servera rešava se pitanje skladištenja pošte, ali ostaje otvoreno pitanje kako zaštiti poruke prilikom same razmene. Trenutno najbolji način zaštite mejlova jeste upotreba PGP (Pretty Good Privacy) sistema za kriptovanje i dekripciju.

PGP sistem koristi dva ključa za slanje i primanje poruke. Privatni ključ se čuva i ne deli ni sa kim, dok se javni ključ daje svakome ko želi da stupi u kriptovanu komunikaciju.

Poruka se kriptuje uz pomoć javnog ključa osobe kojoj je namenjena, kako bi se sadržaj poruke zaštitio u slučaju presretanja prilikom slanja. Dekripcija poruke vrši se privatnim ključem.

PGP se može primeniti na više načina; najjednostavnija upotreba je preko mejl klijenta Mozilla Thunderbird i softverskog dodatka (plugin) za ovu aplikaciju, Enigmail.

Thunderbird je mejl klijent otvorenog koda, program je dostupan na sledećoj adresi:

https://www.mozilla.org/en-US/thunderbird/.

Enigmail je dodatak za Thunderbird koji omogućava jednostavnu primenu PGP kriptovanja.

TOOL BOX

- Za korišćenje Enigmail-a, na Windows OS potrebna je instalacija gpg4win (GNU Privacy Guard for Windows) softvera koji u sebi sadrži PGP algoritme. Softver se može preuzeti sa adrese: **http://www.gpg4win.org/**
- Nakon uspešene instalacije gpg4win-a, potrebno je instalirati Enigmail u Thunderbird-u. To se može uraditi u Thunderbird Menu > Add-ons (u Search Box napišite Enigmail).
- U zavisnosti od verzije operativnog sistema i dodatnog softvera koji je instaliran na računaru, moguće je da program zahteva instalaciju i dodatnih alata, ali su te instalacije jako jednostavne.
- Nakon instalacije Enigmail-a, treba ga konfigurisati: Thunderbird Menu > Enigmail > Setup Wizard. Za većinu korisnika najbolji izbor je I prefer standard configuration > Next
- I want to create a new key pair for signing and encrypting my email > Next. U ovom koraku birate user (svoju mejl adresu) za koju ćete generisati ključeve i unosite Pass Phrase.
- Kada se generišu ključevi, mora se generisati i Revocation Certificate, koji služi za povlačenje ključeva ako je u nekom momentu to potrebno. RC se čuva na bezbednom mestu. Finish.

CHAT

PGP ima svoju primenu i u kriptovanju kratkih poruka (chat) i jednostavno se koristi u aplikaciji Pidgin sa dodatkom OTR (Off The Record).

PIDGIN podržava većinu chat usluga kao što su AIM, Google-Talk, IRC, MSN, Yahoo itd. Takođe podržava i XMPP (Extensible Messaging and Presence Protocol) koji je verovatno najbolje rešenje za privatnu razmenu kratkih poruka.

DUCKDUCKGO, pretraživač koji štiti privatnost svojih korisnika, ima svoj XMPP server koji je besplatno dostupan za korišćenje. Više o tome možete saznati ovde: https://duck.co/blog/post/4/xmpp-services-at-duckduckgo

Aplikacija Pidgin se može preuzeti ovde: **https://pidgin.im/download/.**

HOSTING I DOMEN

Hosting provajder na svojim serverima pohranjuje sve podatke koji čine jedan portal i vodi računa o tome da on bude dostupan na mreži. Domen je registrovana jedinstvena URL adresa koja upućuje na sajt. Domen i hosting mogu i ne moraju biti deo istog paketa usluga.

Organizacije mogu da odaberu da li će svoj sajt hostovati u zemlji ili u inostranstvu. Prilikom izbora, treba voditi računa o poslovanju i bezbednosti:

HOSTING U SRBIJI

- Može se neposredno izvršiti uvid u kvalitet i bezbednost server sale provajdera gde se sajt nalazi
- Veća dostupnost tehničke podrške koja ne zavisi samo od prijave i onlajn komunikcije
- Likvidnost i reputacija hosting provajdera se mogu proveriti u vlastitoj zajednici
- Nema rizika od primene regulative vezane za iznošenje podataka iz oblasti zaštite podataka o ličnosti
- Ako je sajt koji je namenjen domaćoj publici pod DDoS napadom iz inostranstva (što je najčešće slučaj) privremenim blokiranjem inostranih IP adresa može ostati stabilan i dostupan domaćim korisnicima

HOSTING U INOSTRANSTVU

- Sajt je izvan jurisdikcije nadležnih državnih organa
- Na hosting se ne primenjuje domaća legislativa, pa se pravni i administrativni postupci vezani za uklanjanje sadržaja najčešće ne mogu sprovesti bez saglasnosti vlasnika sajta i servera

U tehničkom smislu postoje četiri vrste hostinga:

- Shared hosting je hosting po principu deljenja resursa. Različiti sajtovi koji se nalaze na zajedničkom serveru dele procesor, brzinu protoka, prostor na disku itd. To znači da ukoliko neki od sajtova na shared hostingu ima povećan broj pristupa, protok podataka kod ostalih sajtova na istom serveru biće sporiji. Takođe, ukoliko je jedan od sajtova napadnut, relativno je velika verovatnoća da su i ostali sajtovi na tom serveru kompromitovani.
- VPS – Virtual Private Server je hosting gde svako raspolaže svojim resursima. Tehnički, na jednom fizičkom serveru podiže se više virtuelnih servera i svako od njih raspolaže određenim resursima koje ne deli sa drugima; takođe, ukoliko je jedan od virtuelnih napadnut, integritet ostalih virtuelnih servera nije kompromitovan.
- Dedicated Server ili namenski server je vrsta hostinga gde je samo jedan sajt hostovan na fizičkom serveru, odnosno korisniku je dodeljeno ekskluzivno pravo pristupa mašini i on njome raspolaže kako hoće, može da podiže virtuelne servere i da ih koristi za različite namene, veb hosting, mejl, skladištenje podataka (data storage) i drugo.
- Cloud hosting je hosting na više servera koji su povezani da funkcionišu kao jedan, što doprinosi decentralizaciji sistema, a samim tim i boljem integritetu. U slučaju kvara na jednom od servera, ostali preuzimaju njegovu ulogu pa se problem neće odraziti na rad sajta.

Deljeni (shared) hosting se ne preporučuje u slučajevima kada sajt čine aktivni sadržaji koji se relativno često menjaju i kada broj posetilaca varira. Dedicated hosting i Cloud hosting su bolja rešenja, ali je njihova cena malo veća. Konačno, odabir opcije zavisi od potreba organizacije.

Tehnička podrška je jedan od najbitnijih segmenata usluge hostinga jer u slučaju da nešto pođe po zlu ova služba je tačka za kontakt koja mora biti potpuno kooperativna kako bi se problem što pre rešio. Poželjno je odabrati kompaniju čija je služba tehničke podrške operativna danonoćno, svakog dana u nedelji.

Iako je sav sadržaj i saobraćaj na internetu praktično virtuelan, ipak su u osnovi svega stare dobre mašine. Zato je važno proveriti i kakav hardver koristi hosting kompanija.

Tehničke specifikacije paketa čine, konačno, najbitniju karakteristiku i poželjno je da one budu skalabilne, odnosno da se mogu prilagoditi i nadograđivati u skladu sa promenljivim potrebama organizacije.

Dobar hosting takođe podrazumeva decentralizaciju. Ne preporučuje se da se isti server ko-

risti za hostovanje sajta i kao mejl server ili data centar. Veb server mora da bude dostupan sa javnog interneta, dok bi dostupnost data centra sa javnog interneta bio ozbiljan bezbednosni problem. Ukoliko postoji potreba da se podacima koji se nalaze u data centru pristupa na daljinu, za to je najbolje koristiti VPN usluge.

Na Internetu postoje portali za poređenje hosting paketa:

- Hosting.rs (http://hosting.rs/) - za domaće provajdere·
- HostMonk (http://www.hostmonk.com/)
- Web Hosting Reviews (http://whreviews.com/)

TRAJNO BRISANJE PODATAKA

Konvencionalno brisanje podataka sa računara nije efikasno rešenje za trajno brisanje, jer postoje načini da se izbrisani podaci povrate uz pomoć posebnog softvera. Rešenje za ovaj problem su programi koji kompleksnim algoritmima za razlaganje podataka prave od dokumenata digitalnu "kašu" koja se više nikako ne može vratiti u prvobitan oblik.

Eraser je aplikacija za Windows koja trajno briše dokumenta sa diska. Dostupna je na sledećoj adresi: http://download.cnet.com/Eraser/3000-2092 _ 4-10231814.html

Shredder je aplikacija za Mac računare koja obavlja istu funkciju kao Eraser. Dostupna je na sledećoj adresi: https://www.apple.com/downloads/dashboard/business/shredder.html

Što se tiče standardnih nosača podataka (CD, DVD), najelegantniji način za njihovo trajno uništavanje jeste upotreba specijalnog šredera koji pored papira može da uništava i diskove. Metode za fizičko uništavanje hard diska koje se mogu naći na mrežama, gde se disk stavlja u kiselinu ili se spaljuje, izuzetno su opasne - hard diskovi sadrže različite vrste štetnih hemikalija, koja mogu izazvati otrovna i zapaljiva isparenja. Rizici po zdravlje suviše su veliki za ovako banalne potrebe.

Ukoliko se stara oprema sprema za prodaju ili se neki hard disk odredi za bacanje, biće mu neophodno dubinsko čišćenje čak i ako je pokvaren. Softver koji to radi vrlo efikasno jeste Darik's Boot and Nuke. To je program koji se može pokrenuti sa USB memorije, pa čak i sa flopi disketa koje neki stari uređaji još uvek koriste.

Darik's Boot and Nuke je dostupan na sledećoj adresi:

Darik's Boot and Nuke je dostupan na sledećoj adresi:

http://download.cnet.com/Darik-s-Boot-and-Nuke-for-floppy-disks-and-USB/3000-2094 _ 4-10911312.html

Dobra praksa upućuje da se prilikom bacanja stare opreme - nakon što je poseban softver izvršio dubinsko čišćenje diskova - oprema rasklopi kako bi se uništili ulazi i polomili pinovi na priključcima.

KRITIČNE TAČKE U SISTEMU I NAJČEŠĆI OBLICI SAJBER NAPADA

KRITIČNE TAČKE

Svaka platforma ima nekoliko tačaka koje su najčešće mete napada. Ukoliko veb developer obrati pažnju na ove zone pri kreiranju portala, bitno će smanjiti rizike po sadržaj i neometan pristup sajtu.

Kontakt forme, ankete i drugi segmenti sajta gde čitaoci mogu da unose neke svoje parametre, svakako su najrizičnija mesta jer omogućavaju direktan pristup sistemu. Ukoliko nisu neophodne za rad sajta, od kontakt formi je pametno odustati, dok se ankete mogu ograničiti na jedan unos po IP adresi. Interaktivan odnos sa čitaocima može se razvijati na zasebnom prostoru koji nije u direktnoj vezi sa samim sajtom.

Baza podataka je takođe jedan od rizičnijih delova sajta. Kroz slanje nelogičnih i kompleksnih upita bazi može doći do njene blokade, čime se čitaocima onemogućava pristup sajtu. Rešenje je u strogoj validaciji svakog unosa u bazu i onemogućavanju nelegitimnih upita kroz URL adresu ili na neki drugi način.

Besplatan softver trećih lica (third-party) koji se instalira na platformu da bi se učinila zanimljivijom često može da predstavlja dodatni rizik. Ovaj softver najčešće ima oblik različitih tema ili drugih objekata koji unapređuju funkcionalnost i izgled sajta, ali može sadržati maliciozni kod ili neki bezbednosni propust koji ugrožava integritet sajta. Zbog toga je važno da se uvek koristi samo softver

kredibilnih izvora, odnosno softver za koji postoji dovoljan broj pozitivnih recenzija na mreži.

NAJČEŠĆE VRSTE NAPADA

U najopštijoj podeli, napadi mogu biti izvedeni bez direktnog pristupa serveru ili im je pristup serveru neophodan.

U prvoj grupi su uglavnom napadi kojima je najvažniji cilj da onemoguće pristup sadržaju sajta. Postoji više načina da se obori server, a najčešće se koristi DDoS (Distributed Denial of Service) napad. To znači da ogroman broj računara istovremeno šalje zahteve za pristup napadnutom serveru, koji ne može da odgovori na sve upite i jednostavno prestaje da radi. Nakon što napad prestane, u većini slučajeva server i sajt rade normalno.

Ubacivanje koda (Code Injection) je sofisticiranija vrsta napada, kada se maliciozni kod ubacuje kroz neku otvorenu formu sajta ili kroz URL. Cilj napada je podsticanje baze ili drugog dela sajta da izvršavaju operacije koje nemaju nikakav vidljiv rezultat, ali zauzimaju resurse servera dok ga ne preplave aktivnostima i tako ga ugase. U pojedinim slučajevima, posle ovih napada sajt postaje neupotrebljiv, pa se sadržaj obnavlja poslednjom sačuvanom kopijom. Redovno pravljenje rezervne kopije sajta s pravom se smatra elementarnom bezbednosnom procedurom.

Trojanci koji se unose u sistem društvenim inženjeringom prvi su na listi kada je reč o brojnosti neke vrste napada. Korisnik najčešće pokupi zarazu na opskurnim veb sajtovima gde nesmotreno prihvati upozorenje da je zaražen i aktivira lažni antivirus. Na taj način se godišnje izvrši stotine miliona hakerskih napada, što trojance stavlja u nenadmašivu prednost u odnosu na ostale hakerske napade. Najbolja zaštita od ovakve vrste napada je edukacija i informisanost o savremenim oblicima pretnji. U organizacijama se ovaj problem na neki način rešava filtriranjem sajtova kojima se može pristupiti sa kompjutera u lokalnoj mreži.

Računarski crvi su programi koji sami sebe umnožavaju, koristeći računarske mreže za prenos na druge računare, najčešće bez učešća čoveka. Mogu stići kao prilog u mejlu, a njihovo delovanje omogućavaju bezbednosni propusti u operativnom sistemu. Najbolja zaštita od napada crva jesu antivirusni softveri i kvalitetne lozinke. Druge dobre metode su i zaštitni zidovi (firewall), neotvaranje sumnjivih mejlova i redovno obnavljanje softvera.

Napadi kojima je potreban pristup serveru mahom su komplek-

sniji i ozbiljniji, a za cilj imaju krađu podataka, izmenu sadržaja, plasiranje lažnog sadržaja i onemogućavanje pristupa sadržaju. Ovi napadi su složeni jer napadač mora da probije sve mere zaštite postavljene na serveru da bi došao do pojedinih lozinki, kodova za pristup i slično. Takođe zahtevaju veću stručnost napadača.

ODJAVNI TEKST

Ovaj vodič predstavlja samo uvod u složenu priču o digitalnoj bezbednosti. Bezbednost nije sastavni deo sajber prostora, za nju su neophodna konstantna ulaganja. Informacioni sistem jedne organizacije bezbedan je onoliko koliko je bezbedan najslabije obezbeđeni računar unutar sistema.

Poštovanjem prosečnih standarda digitalne bezbednosti eliminiše se znatan deo pretnji u digitalnom okruženju.

Posvećena informisanju i edukaciji u oblasti prava i bezbednosti na internetu, SHARE Fondacija u okviru svojih redovnih aktivnosti organizuje multidisciplinarne treninge dizajnirane za različite aktere i organizacije, kombinujući pravne i tehničke aspekte upravljanja rizicima u digitalnom okruženju.

Sva izdanja SHARE Fondacije dostupna su na našim platformama:

www.shareconference.net

www.labs.rs