ABC VARNOSTI ZA LASTNIKE SPLETNIH STRANI

si·cert
VARNI NA INTERNETU
register.si

ABC VARNOSTI ZA LASTNIKE SPLETNIH STRANI

V primeru težav se lahko obrnete na:
SI-CERT - *www.cert.si*
Varni na internetu - *www.varninainternetu.si*

VSEBINA

PREDSTAVITEV NA SPLETU

Internet je del našega vsakdana. Meja med realnim in virtualnim svetom je vse bolj zabrisana. Večina podjetij se predstavlja na spletu, mnoga omogočajo tudi spletno nakupovanje. Različna društva splet izkoriščajo za komunikacijo in sodelovanje s svojimi člani, kot posamezniki pa lahko svoje vtise in mnenja hitro predstavimo svetu v svojem spletnem dnevniku (blogu). Ob vseh prednostih spleta pa ne smemo pozabiti tudi na pasti in nevarnosti.

Na kaj vse moramo biti pozorni in kako se težavam na spletu izognemo? Spletno mesto vam običajno postavijo zunanji partnerji, vi pa ste odgovorni za njegovo delovanje, zato morate ohraniti nad njim nadzor in skrbeti za njegovo vzdrževanje.

Vodič podaja nekaj koristnih informacij, če spletno predstavitev že imate ali svoje spletno mesto šele načrtujete. Nastal je v sodelovanju s programom ozaveščanja **Varni na internetu** nacionalnega odzivnega centra za omrežne incidente **SI-CERT** in nacionalnega registra slovenskih domen **Register.si**, ki skrbi za infrastrukturo delovanja slovenskega spleta.

VARNI NA INTERNETU si·cert register.si

Spletno mesto vam postavijo drugi, vi morate ohraniti nadzor in nositi odgovornost.

IZBIRA PONUDNIKA GOSTOVANJA IN IZVAJALCA

Zanesljiv partner

Izberite zanesljivega in odzivnega ponudnika. Na vašo odločitev naj ne vpliva zgolj cena paketa, ampak razmislite, kaj vam bo res pomembno. Morda to, da je ponudnik samo nekaj ulic stran? Vas zanima samo velikost strežnika in povezave ali tudi dodatne storitve, ki jih ponuja?

Faze postavitve spletnega mesta:

(1) NAČRTOVANJE SPLETNEGA MESTA

Kaj želite predstaviti? Zgolj kontaktne podatke ali bogato spletno mesto s katalogom in morda celo spletno trgovino? Od tega je odvisna odločitev o spletnem sistemu za upravljanje z vsebinami. Manjše kot so vaše zahteve, enostavnejši sistem lahko izberete. Bolj ko je ta kompleksen, več vzdrževanja bo zahteval. Med najpogostejše **sisteme za upravljanje z vsebinami oz. Content Management System (CMS) spadajo**: Wordpress, Joomla in Drupal. Osnovno predstavitev lahko izvajalec naredi že v samem HTML-jeziku.

Prijateljev sin

V manjših podjetjih ali društvih velikokrat izberejo znance za oblikovanje in izdelavo spletnega mesta. Tak "prijateljev sin" se sicer spozna na računalnike, bo pa morda naslednje leto odšel na študijsko izmenjavo v tujino ravno, ko bo vam spletno mesto "crknilo". Priložnostni izdelovalec spletnih mest morda pozna le eno samo platformo ter se ne more in ne zna prilagoditi vašim potrebam.

Dejstvo je: dnevi "garažnih" internetnih mojstrov so minili, spletnega mesta se morate lotiti z ustrezno profesionalno podporo.

(2) POSTAVITEV SPLETNEGA MESTA

Spletno mesto boste "postavili" na internet pri enem od **ponudnikov gostovanja**. Pri izbiri naj kriterij poleg cene predstavljajo tudi:

1. zadovoljstvo drugih strank pri ponudniku,
2. dosegljivost ponudnika – kako in kdaj lahko kontaktirate z njim v primeru težav,
3. ali je na voljo redno varnostno kopiranje (backup) podatkov in njihova obnova v primeru težav,
4. ali imate možnost izbrati pakete z dodatno zaščito spletnega mesta in kaj ta zaščita vsebuje (na primer zaznavo nepooblaščenega dostopa in obrambo pred DoS-napadi).

Z zakupom spletnega strežnika ste najeli poslovne prostore na internetu. Način poslovanja in skrb za varnost dokumentacije v njih je vaša naloga. Vašo pisarno redno čistite, urejate dokumentacijo v njej, zamenjate pregorele žarnice in jo zaklepate. Podobne vzdrževalne naloge vas čakajo na spletu. Ni nujno, da vse opravljate sami, zelo verjetno se boste za večino nalog dogovorili z zunanjim izvajalcem. Le-ta mora imeti ustrezna znanja in izkušnje. Mnoge težave spletnega poslovanja so posledica tega, da se udeleženci ne zavedajo, za kaj vse morajo poskrbeti.

Glede na zahteve svojega spletnega mesta izberite pri ponudniku gostovanja najprimernejši paket.

Doma ali na tujem?

Internet je zabrisal meje, zakaj ne bi gostovanja najeli na tujem? Predvsem dobro razmislite, kaj za določeno ceno dobite. Brezplačnih gostovanj se izogibajte, saj ne nudijo podpore v primeru težav (pa čeprav gre za Google). Kako boste reševali zaplete med vami in ponudnikom v Nemčiji ali ZDA? Pri domačem ponudniku gre to praviloma gladko in hitro. Strežniki izven EU so lahko problematični tudi z zakonskega stališča, če na njih hranite osebne podatke.

(3) VZDRŽEVANJE SPLETNEGA MESTA

Najpogostejši vzrok za težave na spletnem mestu je slabo ali neobstoječe vzdrževanje. **Če zanj ne poskrbite, je samo vprašanje časa, kdaj bo prišlo do takšnega ali drugačnega zapleta.** Odpravljanje posledic zlorabe spletnega mesta bo terjalo določen čas in denar, nedostopnost vaše strani ali spletne trgovine pa povzroči tudi izgubo strank, poslovno škodo in prav gotovo ne prispeva k vaši dobri podobi. Splet je dinamično okolje in njegovemu razvoju boste morali slediti tudi s svojim spletnim mestom.

Če imate v podjetju svoje IT-osebje, se seveda oni seznanijo s sistemom za upravljanje z vsebinami in prevzamejo skrb za vzdrževanje. Sicer se morate dogovoriti bodisi s svojim izdelovalcem spletne strani, ponudnikom gostovanja bodisi s tretjim partnerjem. Vsekakor naj za redno vzdrževanje spletnega mesta skrbi zanesljiv in strokoven izvajalec.

200 pohekanih na mesec

Med decembrom 2012 in majem 2013 je SI-CERT obravnaval **1300 primerov slovenskih spletnih mest podjetij**, ki so doživela "razobličenje" spletne strani: tujec jim je vdrl v strežnik in zamenjal vstopno stran s svojim sporočilom. V nekaterih primerih je vdiralec strežnik tudi izkoriščal v svoje kriminalne namene. Vsi ti primeri so posledica nevzdrževanja sistema za urejanje vsebin.

Vzdrževalna dela:

- preverjanje delovanja spletnega mesta (dnevno)
- spremljanje novic o novostih spletne platforme in operacijskega sistema (tedensko)
- nadgradnje spletne platforme (mesečno in obvezno ob kritičnih napakah)
- ažuriranje kontaktnih podatkov za domeno (po potrebi oz. vsaj 1x na leto)

Je kdo doma?

Ni nujno, da boste vi tisti, ki boste prvi opazili zlorabo svojega spletnega mesta. Obvestilo o varnostnem incidentu vam bomo morda posredovali iz odzivnega centra SI-CERT in takrat moramo hitro najti vaš elektronski naslov. Vaše spletno mesto je lahko v celoti izbrisano in zato kontaktnih podatkov na vaši spletni strani ni moč videti. V takem primeru je pomembno, da hitro pridemo do vas. Običajno se naslanjamo na register nosilcev slovenskih domen. **Še veste, kateri kontakt ste navedli pri registraciji domene?**

DOMENA

Domena je naslov vaše spletne predstavitve, lahko bi rekli, da je pomemben inventar vašega podjetja ali društva. Tudi pravilno ravnanje z domeno pripomore k varnosti na spletu.

Najprej nekaj osnovnih pojmov:

Register je organizacija, ki je skrbnik vrhnje domene. Skrbi za bazo registriranih domen, za delovanje vrhnjih domenskih strežnikov, razvija in vzdržuje sistem za registracijo domen in opravlja druge storitve, vezane na vrhnjo domeno. Za vsako vrhnjo domeno obstaja en register.

Registrar ima dostop do sistema za registracijo domen in opravlja registracijo, podaljšanje in druge storitve, vezane na domeno, v imenu svojih strank. Registrarji lahko svojim strankam ponujajo domene pod različnimi končnicami, vsak register ima lahko več registrarjev.

Nosilec je tisti, ki je domeno registriral in za določeno obdobje pridobil pravico, da z njo razpolaga in jo uporablja kot spletni in/ali elektronski naslov.

Domeno lahko registrirate tudi pod katero drugo vrhnjo domeno. Navodila za registracijo boste našli na spletu. Priporočila in navodila v nadaljevanju sicer veljajo za slovenske domene, vendar so splošno uporabna tudi za domene pod drugimi končnicami.

Na kaj morate biti pozorni pri registraciji domene:

1. **Vi ste nosilec domene.** Ker nosilec domene lahko edini upravlja z domeno, poskrbite, da bodo podatki o nosilcu pravi. Ne dovolite, da se kot nosilec vpiše izdelovalec vaše spletne strani. Če že, naj se vpiše le kot tehnični kontakt. Kaj hitro se lahko zgodi, da boste po nekaj letih ugotovili, da je vaša **spletna identiteta, na kateri temelji npr. celotno poslovanje podjetja**, v rokah nekoga, s katerim ste že zdavnaj prekinili poslovne stike. Poleg **naziva in naslova nosilca** je bistveno, da je ob registraciji **naveden delujoč elektronski naslov**, po možnosti takšen, do katerega ne dostopajo vsi zaposleni. Prek elektronskega naslova nosilca namreč poteka vsa uradna komunikacija med registrom in nosilcem domene. **Kdor ima dostop do tega naslova, lahko potrdi izbris domene, zamenjavo registrarja ali pa celo prenos domene na nekoga drugega.**
2. **Tehnični kontakt ve, kako stvari delujejo.** Tehnični kontakt za domeno naj bo nekdo, ki zna postaviti vaše spletno mesto, urejati vpise v DNS-strežnike in se bo znal odzvati na sporočila o tehničnih težavah in o morebitnih zlorabah vašega spletnega mesta.
3. **Izbira registrarja.** Registrarjev za domeno .si je veliko. Pri izbiri pravega premislite, kaj želite: osebni kontakt, svetovanje, pomoč ali morda enostavno, avtomatizirano registracijo; paleto dodatnih storitev ali telefonski klic, če ste domeno pozabili podaljšati. Vsa opravila z domenami (npr. podaljšanje, spremembo podatkov, vpis domenskih strežnikov ...) boste opravljali **izključno prek registrarja**, zato preverite, kako ti postopki pri izbranem registrarju potekajo in kakšna je registrarjeva odzivnost.

Ko domeno imate, nanjo ne smete povsem pozabiti.

Domeno registrirate za obdobje od enega do petih let, odvisno od dogovora z registrarjem. Po poteku tega obdobja jo je treba **podaljšati**, kar bo v vašem imenu uredil registrar. V nasprotnem primeru bodo vaša spletna stran in vsi elektronski naslovi pod poteklo domeno **prenehali delovati**. Domena vas bo "čakala" še 30 dni, nato pa jo bo lahko registriral kdo drug. Če ste pozabili, do kdaj je vaša domena registrirana ali celo to kdo je vaš registrar, lahko vse podatke preverite prek spleta na "WHOIS" spletni strani registra: **register.si/whois**. Bodite pozorni tudi na podatke o nosilcu domene, ki jih izpiše WHOIS. Če niso pravilni, o tem takoj obvestite svojega registrarja. **Posledica netočnih podatkov je lahko izbris domene!**

Kaj storiti, če ste ugotovili, da je "vašo" domeno pod .si registriral nekdo drug? Če lahko pokažete,

1. da je domena enaka ali zelo podobna vaši blagovni znamki ali nazivu podjetja,
2. da nosilec nima pravno priznanega interesa glede registrirane domene in
3. da je domena registrirana ali se uporablja v slabi veri,

lahko pri registru sprožite domenski spor s pomočjo postopka **alternativnega reševanja domenskih sporov** (ARDS).

(!) Nosilci se morate zavedati, da ste tudi vi odgovorni, da z izbrano domeno ne kršite zakonov in pravic drugih oseb.

Zakaj domena pod nacionalno končnico .si?

Prednost .si domene s stališča varnosti je gotovo ta, da registrar posluje v slovenskem jeziku in istem časovnem pasu, kar olajša komunikacijo in omogoča hitro odzivnost pri zapletih in težavah, za vse vpletene pa velja slovenska zakonodaja.

ZAKONODAJA

Odgovornost za vsebine na vašem spletnem mestu nosite vi. Če vdiralec na vaše spletno mesto naloži orodja, s katerimi povzroča škodo drugim uporabnikom na spletu, ste lahko soodgovorni tudi vi, če ob obvestilu o tej dejavnosti ustrezno ne ukrepate.

Splet ureja tudi slovenska zakonodaja. Posamezne zakone in relevantne člene si lahko ogledate na **www.cert.si/zakonodaja**, izpostavimo pa nekaj področij, ki jih kot lastnik spletnega mesta morate poznati.

ODGOVORNOST

Zakon o elektronskem poslovanju na trgu (ZEPT, 11. člen) določa, da ponudnik gostovanja ni odgovoren za podatke, ki jih vi kot njegova stranka naložite na strežnike, dokler se ne zaveda, da gre morebiti za protipravno dejavnost. Takoj, ko mu je ta znana, pa mora odstraniti ali onemogočiti dostop do teh podatkov. **Ob morebitnih pritožbah glede vsebine, ki je naložena na vašem spletnem mestu, ima ponudnik torej jasno zakonsko dolžnost, da ob pritožbi dostop do njega onemogoči.** Poleg tega lahko ponudnik v svojih splošnih pogojih določi dodatna pravila, ki jih morate pri uporabi njegovih storitev upoštevati.

OGLAŠEVANJE IN SPAM

Pošiljanje oglasov brez vnaprejšnjega soglasja naslovnika je v nasprotju s slovensko zakonodajo. Področje neželene elektronske pošte (spam) urejajo kar štirje zakoni: Zakon o varstvu potrošnikov, Zakon o elektronskem poslovanju na trgu, Zakon o

elektronskih komunikacijah in Zakon o varstvu osebnih podatkov. **Izgovor, da ste naslove dobili na javno dostopnih spletnih straneh, ni dovolj. To ni soglasje za spam!**

INTELEKTUALNA LASTNINA

Skupaj z izdelovalcem spletnega mesta morate poskrbeti za to, da imate za uporabo vsebin ustrezna dovoljenja. **Če ste sliko našli "na Googlu", to nikakor še ne pomeni, da jo lahko tudi uporabite.** Lahko je v tuji lasti in če je javno objavljena, spet ne pomeni, da njen avtor vsem dovoli njeno prosto uporabo! Nekatere vsebine se lahko prosto uporabljajo, nekatere pod določenimi pogoji (primer: Creative Commons), sicer pa morate dovoljenje dobiti od nosilca pravic.

SLEDENJE UPORABNIKOM IN PIŠKOTKI

Spletni piškotki so majhne tekstovne datoteke, ki jih spletni strežnik ob obisku ponudi brskalniku obiskovalca in se običajno shranijo na njihov računalnik ali mobilno napravo, ob poznejših obiskih pa se shranjeni piškotek iz brskalnika ponovno pošlje strežniku. Piškotki se uporabljajo za shranjevanje nastavitev, vodenje seje posameznega uporabnika, razlikovanje med uporabniki in za njihovo sledenje na spletišču (lahko tudi med več spletišči). **Če boste na spletnem mestu uporabljali piškotke, morate v skladu z Zakonom o elektronskih komunikacijah (ZEKom-1) uporabnike obvestiti** o vrsti piškotkov, ki jih uporabljate in pridobiti njihovo soglasje.

Več o piškotkih si preberite v **smernicah Informacijskega pooblaščenca**.

OBRAVNAVA OSEBNIH PODATKOV

Če na strežniku hranite ali obdelujete osebne podatke, morate v skladu z Zakonom o varstvu osebnih podatkov **zbirke osebnih podatkov prijaviti Informacijskemu pooblaščencu**. Če boste najeli strežnik v tujini, preverite, ali je izvoz osebnih podatkov v tisto državo dovoljen (v EU-članice je izvoz podatkov dovoljen, v ZDA pa le v podjetja, ki so podpisala ustrezen sporazum). Pri Informacijskem pooblaščencu se pozanimajte o tem, prav tako preverite, ali je treba s ponudnikom gostovanja podpisati pogodbo o obdelavi osebnih podatkov.

MOŽNE ZLORABE

Posledice vdora:

1. moteno delovanje ali izpad spletnega mesta,
2. izguba, sprememba ali kraja podatkov,
3. ogrožanje obiskovalcev vašega spletnega mesta,
4. blokada vaše elektronske pošte,
5. blokada vašega spletnega mesta na internetu.

KAKO DO VDORA PRIDE?

Najpogosteje vdiralec najde varnostno luknjo v nevzdrževanem sistemu za upravljanje vsebin ali strežnika. Dostop lahko pridobi tudi s krajo vašega gesla ali ugibanjem, če je geslo enostavno. Nekaj najpogostejših vrst vdorov in zlorab naštevamo v nadaljevanju.

RAZOBLIČENJE

Podoba spletnega mesta je spremenjena. Razobličenje oziroma defacement je "grafitiranje" vašega spletnega mesta, prek katerega želi napadalec izraziti svoje mnenje, bodisi osebno bodisi politično, ali pa le pustiti svoj podpis. Obiskovalec vašega spletnega mesta bo namesto predstavitve vašega podjetja videl napis: "Hacked by Hmei7" ali pa proglase o svobodni Palestini.

PHISHING - KRAJA GESEL

Napadalec izkoristi **vaše spletno mesto za postavitev lažne kopije** npr. spletne strani banke in prek vašega strežnika skuša ukrasti gesla ter nato tudi denar njenih komitentov. Napadalci uporabljajo phishing tehniko tudi za krajo drugih podatkov: gesel elektronske pošte, številk kreditnih kartic, uporabniških računov ipd. Končne žrtve napada napadalec na phishing spletno stran v večini zvabi prek prirejenega elektronskega sporočila, v katerem jih obvešča, da morajo zaradi različnih razlogov ponovno vnesti svoje podatke, povezava pa vodi na podtaknjeno phishing spletno stran na vašem strežniku.

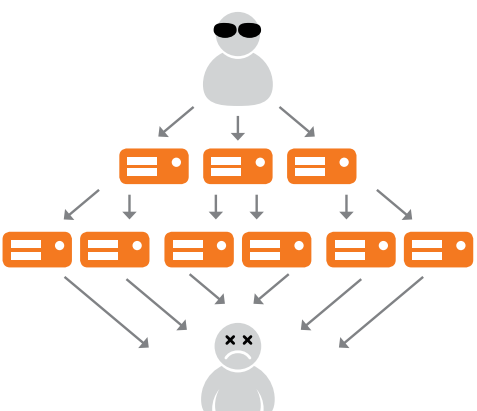
NAPAD S ŠKODLJIVO KODO

Vaše spletno mesto napadalci izkoristijo za širjenje zlonamerne kode: virusov, trojanskih konjev in računalniških črvov. Napadalec na vašo spletno mesto odloži programsko kodo, ki poskuša izrabiti ranljivosti v brskalniku obiskovalca oziroma v dodatkih (vtičnikih, angl. "plug-in") brskalnika. V tem primeru ste pravzaprav **soudeleženi pri okužbi računalnikov vaših spletnih obiskovalcev**. Okužbe imajo lahko za posledico krajo podatkov z okuženega sistema ali finančno oškodovanje. **Zato morate ukrepati takoj, ko ugotovite, da se vaš spletni strežnik uporablja za širjenje škodljive kode.**

ONEMOGOČANJE SPLETNIH MEST

Vaše spletno mesto je nedosegljivo zaradi porazdeljenega napada (DDoS, Distributed Denial-of-Service, tudi "dosanje"). Loti se vas lahko izsiljevalec iz oddaljene države, jezna stranka ali bivši zaposleni, celo konkurenca. Če je bil napad najavljen, shranite kopijo vse komunikacije in shranite čim več podatkov o prometu, ki ga je bil vaš strežnik deležen.

Lahko se znajdete tudi na drugi strani, ko napadalec vdre v vaš strežnik in ga nato uporablja za napade na druga spletna mesta. Decembra 2012 je bilo nekaj deset slovenskih spletnih strežnikov z nevzdrževanim sistemom za upravljanje vsebin Joomla zlorabljenih s strani napadalcev iz tujine. Ti so po vdoru na strežnike nanje namestili svoje programe, s katerimi so izvajali napade na banke v ZDA.



PRIPOROČENI UKREPI

Tveganja zmanjšate že z nekaj preprostimi koraki: poskrbeti morate za redno posodabljanje spletnega strežnika in nameščenega sistema za urejanje vsebin, pametno izbrati gesla ter prijave na svoj strežnik omejiti na svoje običajne internetne lokacije.

1. **MOČNO GESLO.** Pri izbiri gesla moramo paziti, da le-to ni preveč enostavno oziroma pogosto. Sestavljeno naj bo iz različnih znakov (velike črke, male črke, števila, simboli) in dolgo najmanj osem znakov. Največje varnostno tveganje predstavljajo privzeta uporabniška imena, kot so denimo admin, administrator, in gesla 123456, test123 itd.
2. **ZANESLJIV SISTEM**. Za urejanje spletnega mesta se prijavimo le iz zaupanja vrednih sistemov. Pogoste so namreč zlorabe, ki so posledica prijav iz okuženih javno dostopnih sistemov, kot so na primer cybercafeji oziroma knjižnice.
3. **REDNO POSODABLJANJE.** Z ustreznim spremljanjem in posodabljanjem strežnika in sistema za upravljanje z vsebinami bomo poskrbeli za zaščito pred veliko večino napadov. Vzdrževalec spletne strani mora redno spremljati varnostna obvestila proizvajalca sistema za upravljanje vsebin in vestno nameščati popravke zanj in za vse uporabljene dodatke. Če varnostnih posodobitev ne izvajamo sami, moramo to nalogo zaupati pogodbenemu vzdrževalcu.

Naprednejša spletna mesta, ki hranijo osebne podatke ali izvajajo finančne transakcije (spletne trgovine) je smotrno preveriti z neodvisnim varnostnim pregledom in penetracijskim testom. Varnostni pregled bo dal boljše rezultate, če boste izbrali neodvisno podjetje, ki se redno ukvarja s to dejavnostjo.

Kaj storiti ob napadu ali vdoru v spletno mesto?

Ko opazite, da s spletnim mestom nekaj ni v redu, in sumite na nepooblaščen dostop ali vdor v spletno mesto, opravite naslednje korake:

1. Kontaktirajte s skrbnikom strežnika ali svojim ponudnikom gostovanja, pri katerem imate najet spletni strežnik; poskrbite za zavarovanje dokazov o vdoru: predvsem storilčevih datotek in sprememb na sistemu in dnevniških datotek. Pri tem bodite zelo pozorni, da navedenih datotek ne spreminjate in se ohranijo v celoti skupaj z ustreznimi časovnimi oznakami (čas kreiranja, spreminjanja in dostopa do datoteke).
2. Vdor sporočite na SI-CERT prek elektronske pošte: **cert@cert.si**. V sporočilu opišite znake vdora in vam znane okoliščine vdora. SI-CERT vam bo nudil nadaljnjo pomoč pri preiskovanju vdora, dodatni zaščiti strežnika in bo opravil potrebno komunikacijo z drugimi vpletenimi (to so lahko ponudniki interneta, CERT-centri v tujini in po potrebi tudi organi pregona).

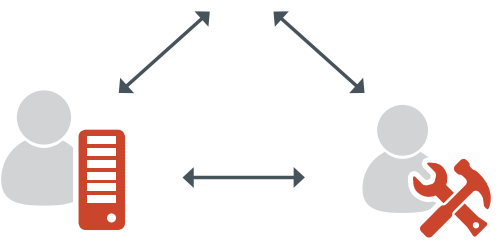
(!) Večina zlorab izvira ravno iz znanih ranljivosti sistemov za upravljanje z vsebinami. **Zato je redno vzdrževanje najpomembnejše. S posodabljanjem zakrpate varnostne luknje.** To delo naj opravlja nekdo, ki se tehnično spozna na vzdrževanje strežnikov in sistemov za urejanje vsebine.

Napadalci ne izbirajo žrtev načrtno. Večino najdejo prek spletnih iskalnikov ali z naključnim preizkušanjem. Šele ko pridejo v vaše spletno mesto, se odločijo, na kakšen način ga bodo najbolj dobičkonosno uporabili: za širjenje škodljive kode, napade na druge, morda pa imate na njem celo določene podatke, ki jih lahko neposredno unovčijo.

RAZDELITEV VLOG

LASTNIK SPLETNEGA MESTA

- je nosilec domene in skrbi za podaljševanje
- je odgovoren za delovanje in vsebino spletnega mesta
- izbere izdelovalca oz. skrbnika spletnega mesta in ponudnika gostovanja



IZDELOVALEC OZ. VZDRŽEVALEC SPLETNEGA MESTA

- je tehnični kontakt pri domeni
- oblikuje in izdela spletno mesto
- skrbi za vpise v DNS-strežnik
- odpravlja napake
- spremlja obvestila in redno namešča popravke sistema za urejanje vsebin

PONUDNIK GOSTOVANJA

- zagotavlja delovanje strežnika
- zagotavlja internetno povezljivost do strežnika
- po dogovoru lahko prevzame skrb za DNS
- prevzame vzdrževanje strežnika, če to storitev ponuja v ustreznem paketu

SEZNAM KONTAKTOV

Na koga se lahko obrnete v primeru težav?

1. Napaka na spletni strani

Najprej se obrnite na izvajalca, ki je spletno mesto postavil in vam ga vzdržuje. Če je potrebno, se bo ta obrnil na gostitelja in preveril, zakaj je do težave prišlo.

2. Nedostopnost spletnega mesta

Obrnite se na vzdrževalca spletnega mesta, ta bo preveril, zakaj je strežnik nedostopen. Če gre za porazdeljen napad na vaš strežnik, se obrnite na ponudnika gostovanja in kontaktirajte z odzivnim centrom za omrežne incidente SI-CERT: **cert@cert.si**.

3. Motnja pri dosegljivosti vaše domene

Če pozabite podaljšati domeno ali pride do napak pri vpisu le-te v DNS-sistem, bo vaš strežnik nedosegljiv. Obrnite se neposredno na registrarja domene ali na svojega vzdrževalca, ki skrbi za vašo domeno.

4. Vdor ali zloraba na spletnem mestu

Kontaktirajte z odzivnim centrom za omrežne incidente SI-CERT: **cert@cert.si**.

TOP 5 TVEGANJ

1. Razobličenje spletnega mesta

Vaše spletno mesto prikazuje sporočilo, kjer se vdiralec hvali, da vas je "pohekal". To ste mu omogočili vi zaradi slabo vzdrževanega spletnega strežnika.

2. Spletno mesto izkoriščajo kriminalci

Po vdoru v vaš spletni strežnik kriminalci namestijo viruse, ki bodo okužili računalnike vaših obiskovalcev. Naložijo lahko svoje programe za izvajanje spletnih napadov na tuje strežnike ali na vaš strežnik namestijo lažne spletne strani za tujo banko (phishing) in prek njih kradejo denar.

3. Kraja osebnih podatkov ali gesel

Z vdorom lahko storilec pridobi dostop do zbirk podatkov, morda tudi osebnih podatkov vaših strank. S phishing napadom lahko kradejo gesla tujim uporabnikom.

4. Izbrisani podatki

Vdiralec vam izbriše podatke na spletnem mestu. Morda to stori konkurenca, odpuščeni delavec, izsiljevalec, ki mu niste želeli plačati "odkupnine", ali nekdo, ki je vdiral prek vašega strežnika naprej in sedaj briše sledi za seboj.

5. Izguba domene

Ker ste na svojo domeno pozabili, je potekla in ne deluje več. Če kontaktni podatki niso ažurni, boste imeli nekaj težav, da jo spet "aktivirate". V najslabšem primeru lahko domeno celo izgubite in jo prevzame nekdo drug.

TOP 5 NASVETOV

1. Poiščite vzdrževalca

Ko postavite spletno mesto, mora nekdo zanj redno skrbeti. Če sami nimate dovolj znanja, morate nalogo vzdrževanja podeliti strokovnemu izvajalcu in zanjo tudi plačati primerno ceno.

2. Cena ni vse

Pri izbiri gostitelja ne glejte samo na najnižjo ceno, ampak tudi na to, kaj gostitelj ponuja, kakšne izkušnje z njim imajo drugi ter ali boste težave lahko hitro rešili. Če je gostitelj v tujini ali ste izbrali brezplačno gostovanje, bo lahko reševanje problemov trajalo dlje časa.

3. Zaščita spletnega mesta

Dostop do spletnega mesta omejite na znane lokacije, redno nameščajte posodobitve za programsko opremo na strežniku in izberite dovolj močna gesla. Pozanimajte se, ali gostitelj ponuja dodatne pakete za zaščito.

4. Varnostne kopije

Redno izdelujte varnostne kopije vsebin vašega strežnika. Poskrbite za beleženje dostopov in napak v dnevniške datoteke. Oboje bo pomembno ob vdoru v vaš strežnik in izgubi ali spremembi podatkov na njem.

5. Ohranite nadzor

Sami ste odgovorni za delovanje strežnika in ko ste obveščeni o zlorabi ali vdoru, se morate ustrezno odzvati. Vi morate biti navedeni kot nosilec domene, da lahko potrjujete spremembe na njej.

ABC VARNOSTI ZA LASTNIKE SPLETNIH STRANI

si·cert

VARNI NA INTERNETU

register.si

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA IZOBRAŽEVANJE, ZNANOST IN ŠPORT