Hic Salta SCAN - HSS

STE VARNI

PRED NAPADI IZ INTERNETA?

Varnostno preverjanje zunanjega omrežja

KAJ VSEBUJE STORITEV HSS

- 2X LETNO VARNOSTNO TESTIRANJE OMREŽJA
- 2X LETNO ENODNEVNO IZOBRAŽEVANJE R&Ž
- 2X LETNO CD R&Ž Z VARNOSTNIMI ORODJI
- POMOČ PRI ODPRAVLJANJU ODKRITIH RANLJIVOSTI
- 1X BONUS SKENIRANJE PO IZBIRI NAROČNIKA
- 25% POPUST PRI NAROČILU NOTRANJEGA TESTIRANJA

POSTOPKI HSS SLONIJO NA INDUSTRIJSKIH STANDARDIH IN PRIPOROČILIH

- OSSTMM
- ISSAF
- PCI DSS
- OWASP
- ISACA
- CHECK

Hic Salta SCAN - HSS

REDNO VARNOSTNO PREVERJANJE ZUNAJEGA OMREŽJA

Varnostni testi so postali neizogibna nuja. Z njimi odkrijemo varnostne pomanjkljivosti in jih nato tudi odpravimo. Vendar, razmere se hitro spreminjajo in to, kar velja danes, že jutri morda ne drži več. Vdiralci, konkurenca pa tudi kriminalci neprekinjeno razvijajo nova orodja in metode, ki jim omogočajo nepooblaščen dostop do vaših sistemov in podatkov. S tem lahko ogrozijo vaše poslovanje. Tudi sistemski administratorji niso nezmotljivi in spremembe v nastvitvah pogosto nehote odprejo pot nepooblaščenim. Izpostavljenost zunanjim grožnjam bistveno zmanjšamo z rednimi varnostnimi preverjanji in izobraževanjem administratorjev. Raziskave kažejo, da dobro varovano okolje odvrača napadalce, ki se raje preusmerijo na iskanje nove, bolj ranljive tarče. S kombinacijo ustreznih tehnologij, ukrepov in primernih nastavitev bistveno zmanjšamo možnost za uspešen napad na našo infrastrukturo.

Hic Saltina storitev HSS prinaša obe bistveni postavki za večjo varnost in zmanjšanje tveganj: redna varnostna preverjanja in redno seznanjanje administratorjev z novostmi.

HSS je ustrezna rešitev za zamnjševanje varnostnih tveganj pred zunanjimi napadi

HSS TEMELJI NA INDUSTRIJSKIH STANDARDIH (OSSTMM, PCI, OWASP)

POSTOPEK

Izkušnje kažejo, da hiter pregled s komercialno programsko opremo za iskanje varnostnih slabosti (t.i. »scannerji«) sicer lahko odkrije marsikatero varnostno pomanjkljivost, v glavnem pa ne izpolni pričakovanj uporabnika, ki se kaj hitro izgubi v obširnih poročilih in množici opozoril.

Le poglobljeno varnostno preverjanje z več komercialnimi in “hekerskimi” orodji in postopki izlušči in razkrije najnevarnejše ranljivosti. Zanje nato predlagamo načine za odpravljanje, v nadaljevanju pa lahko tudi pomagamo pri implementaciji popravkov.

HIC SALTA je v letih izvajanj varnostnih testiranj razvila svojo tehnologijo postopkov, ki pa v veliki meri temelji na priporočilih industrijskih standardov (PCI, ISACA, CHECK, OSSTMM, OWASP).

Naši testi varnostnih sistemov temeljijo predvsem na standardu OSSTMM (Open Source Security Testing Methodology Manual – http://www.isecom.org/osstmm), ki dovolj natančno opredeljuje postopek izvajanja varnostnih testiranj - tako zunanjega kot notranjega omrežja.

Pri varnostnem preverjanju spletnih aplikacij sledimo standardu OWASP (Open Web Application Security Project - http://www.owasp.org), ki prerašča v »defacto standard« za kvaliteten razvoj in testiranje spletnih strežnikov in aplikacij.

METODOLOGIJA HSS

- Pridobivanje osnovnih informacij
- Skeniranje omrežja in sistemov
- Varnostno skeniranje spletnih aplikacij
- Odkrivanje in analiza varnostnih slabosti
- Kontrolirana izraba odkritih pomanjkljivosti
- Definiranje priporočil za odpravo pomanjkljivosti
- Izdelava poročila

POROČILO

Končno poročilo vsebuje naslednje elemente:

- Primerjavo z ugotovitvami prejšnjega varnostnega testiranja (npr. novi sistemi, servisi, aplikacije…)
- Povzetek za vodstvo
- Podrobnosti o posameznih ranljivostih skupaj s priporočili za njihovo odpravo
- CD s poročili posameznih orodij, ki so bila uporabljena za testiranje

Tehničnim strokovnjakom naročnika so, poleg pisnega poročila, rezultati predstavljeni tudi v obliki prezentacije.

LOKACIJA IN ČAS

Testiranje poteka iz lokacije HIC SALTE, prek interneta, v časovnem okviru enega tedna, ki je usklajen z naročnikom. Vsi testi so nedestruktivni in bistveno ne obremenijo naročnikove infrastrukture.

Testiranje je lahko »glasno« (s predhodnim obvestilom oz. dogovorom o času in poteku testiranj) ali »tiho« (brez predhodne najave). Smisel »tihega« testiranja je v preverjanju naročnikovega sistema, da zazna »napad« iz interneta.

PREDMET PREVERJANJ

OSNOVNE INFORAMCIJE:

- Zapisi DNS
- Registrar
- Zapisi A, MX, INFO
- Informacije WHOIS
- Nabor naslovov IP
- E-poštni naslovi
- Informacije, dosegljive prek javnega spletnega strežnika in strežnika FTP
- Spletni iskalniki in uporabniške skupine
- Odkrivanje javnega dostopa do zaupnih informacij (odtekanje informacij)
- Partnerji in druge povezave

OMREŽJE IN SISTEMI:

- Osnovna infrastruktura (usmerjevalniki in požarna pregrada)
- Javno dostopni sistemi (WWW, FTP, SMTP)
- Aktivni sistemi
- Odprta in filtrirana vrata (porti) na dosegljivih sistemih
- Identifikacija operacijskih sistemov
- Delujoči servisi na aktivnih vratih
- Spletne aplikacije (E-trgovina, E-banka,…)

POROČILO

Najpomembnejši rezultat vsakega varnostnega preverjanja je končno poročilo, ki na pregleden in razumljiv način opiše ugotovljene pomanjkljivosti in naročniku tudi predlaga ukrepe, s katerimi jih lahko odpravi ter s tem zmanjša varnostna tevganja.

Dokument vsebuje kratko in jedrnato poročilo za vodstvo (stran ali dve) in podroben tehničen opis odkritih pomanjkljivosti s priporočili za njihovo odpravo. Tudi tehnični del poročila ni predolg, saj bi z obsežnostjo izgubil svojo uporabno vrednost.

Poleg končnega poročila naročniku izročimo tudi zgoščenko z vsemi poročili posameznih orodij, ki so bila uporabljena v okviru testa (dokumenti, ki so običajno dolgi nekaj 100 strani in so namenjeni podrobnejšemu pregledu posameznih ugotovitev).

BONUS – DODATEN TEST (“Kvizko”)

Dodaten pregled na poziv naročnika. “Kvizka” lahko uporabite po spremembi vašega okolja. Naj strokovnjaki odkrijejo pomanjkljivosti pred napadalci.

RAVBARJI IN ŽANDARJI

Eno najpopularnejših izobraževanj s področja računalniške varnosti v Sloveniji. Kot naročniku vam pripada udeležba na spomladanskem in jesenskem terminu.

ORODJA

Orodja za testiranje računalniške varnosti so običajno draga. Za njihovo uporabo so potrebna posebna znanja. Prepustite ta strošek in nalogo varnostnim strokovnjakom. Nekaj orodij, ki jih uporabljamo v okviru storitve HSS:

Qualys
Rapid 7
Nessus
Sandcat
Netsparker
Burp …

TESTIRANJE NOTRANJEGA OMREŽJA

Vas skrbi stanje varnosti notranjega omrežja? Kot naročniku storitve HSS vam pripada 25% popust pri izvedbi varnostnega testiranja notranjega omrežja.

Kaj naročnik pridobi s storitvijo HSS

Naročnik najmanj dvakrat letno dobi odgovor na vprašanje, kako je zavarovano njegovo okolje pred napadi iz interneta. Storitev HSS odkrije pomanjkljivosti tako na omrežni infrastrukturi, sistemih in servisih, kot tudi na aplikacijah, ki omogočajo naročnikove storitve. Naročnik dobi redno potrditev ali so njegove nastavitve opreme in aplikacij primerne s stališča računalniške varnosti, oziroma ali varnostni mehanizmi ustrezno zaznajo nedovoljene aktivnosti na omrežju in sistemih (log datoteke, SIEM, IPS/ IDS,…).

BONUS VARNOSTNO TESTIRANJE

V primeru, da pride do večjih sprememb na infrastrukturnih elementih omrežja ali samih strežnikih in aplikacijah, ima naročnik možnost (enkrat letno, večkrat po dogovoru) naročiti ponovitev varnostnega testiranja. Nekaj primerov sprememb:

- Spremembe DNS
- Prehod na drugega ponudnika ISP
- Uvajanje novega sistema požarne pregrade
- Uvajanje tehnologije VPN
- Nadgradnja oziroma uvajanje nove spletne aplikacije
- Postavitev SIEM ali IPS/IDS sistema …

IZOBRAŽEVANJE “RAVBARJI IN ŽANDARJI”

Upravljavci sistemov in omrežja morajo dobro poznati področje računalniške varnosti, če želimo, da uspešno varujejo svoja računalniška okolja. Za računalniško varnost je značilna velika dinamika s stalnimi spremembami in vedno novimi grožnjami. Zato je potrebno znanje stalno obnavljati.

V okviru izobraževanja “Ravbarji in žandarji” se naročnik dvakrat na leto seznani z novimi trendi na področju računalniške varnosti. Pridobljena znanja o novih grožnjah, orodjih, novostih na področju varnostnih standardov so upravljalcem računalniškega okolja v pomoč pri njihovih dnevno operativnih nalogah. Slušateljem je poleg znanja posredovana tudi zgoščenka z uporabnimi orodji in dokumenti, ki jih lahko uporabijo v svojih okoljih.

ORODJA

Pri varnostnih testih uporabljamo velik nabor različnih varnostnih orodij. Za podjetja nabava večjega števila orodij navadno ni ekonomsko opravičljiva (strošek nabave in potrebno šolanje za uporabo). Storitev HSS vključuje testiranja z najbolj priznanimi orodji za preverjanje računalniške varnosti.

PRIHRANEK PRI VARNOSTNEM TESTIRANJU NOTRANJEGA OMREŽJA

Poleg varnostnega testiranja zunajega omrežja je priporočljivo na podoben način preveriti tudi stanje varnosti notranjega omrežja. V primeru, da se naročnik storitve HSS odloči tudi za izvedbo notranjiga testiranja, mu za to pripada 25% popust.

ZAKAJ HIC SALTA?

V podjetju HIC SALTA d.o.o. se že 15 let ukvarjamo z področjem računalniške in informacijske varnosti. V tem času smo postali zaupanja vreden partner našim strankam, domačim in tujim poslovnim partnerjem, ki je s postavitvijo varnostnih rešitev, svetovanjem, izobraževanjem in drugimi storitvami pomagal najuglednejšim slovenskim podjetjem, organizacijam in bankam pri učinkovitejši, predvsem pa varnejši uporabi informacijske tehnologije.

Pomembno področje delovanja podjetja so različne oblike varnostnih testiranj, ki jih izvajamo v velikem številu slovenskih podjetij, bank in drugih organizacij. Na osnovi dolgoletnih izkušenj na množici testiranj, izobraževanj, partnerstev z najuglednejšimi proizvajalci varnostnih rešitev in varnostnih standardov smo razvili svojo tehnologijo testov. Priporočila, ki jih izdamo na osnovi rezultatov testov, našim naročnikom omogočajo, da izboljšajo varnost svojega IT okolja in zmanjšajo tveganja, ki ogrožajo njihovo dejavnost.

IMATE VARNO IT OKOLJE?

Dovolite da poiščemo ranljivosti, ki lahko ogrozijo delovanje vaših sistemov in aplikacij in vam svetujemo, kako jih odpraviti.

Zaupajo nam mnogi.

HIC SALTA

HIC SALTA d.o.o.

Tbilisijska 85, 1000 Ljubljana

Tel: 01 244 78 22 www.hicsalta.si
Fax: 01 244 78 30 info@hicsalta.si