

Sigurnosni standardi za odabir pružatelja aplikacijskih usluga

1.0 Pregled

Ovaj dokument određuje minimalne sigurnosne kriterije koje pružatelj aplikacijskih usluga (u nastavku ASP) mora zadovoljiti da bi ga poduzeće <> uključilo u odabir. U postupku odabira ASP mora iskazati usklađenost sa standardima koji su navedeni u nastavku. Ponuđač iskazuje usklađenost s uvjetima tog dokumenta na način da pismeno odgovori na SVA pitanja iz stavke broj šest. Služba za sigurnosnu zaštitu (u nastavku InfoSec) će pregledati odgovore na pitanja i predložiti odgovarajuće mjere za područja u kojima sigurnosni kriteriji nisu bili ispunjeni. Suglasnost koju izabire ASP, a daje ju InfoSec, u najvećoj mjeri ovisi o sadržaju odgovora na pitanja iz tog dokumenta.

InfoSec dopunjava sadržaj tog dokumenta te ga mijenja bez prethodnog upozorenja.

2.0 Područje valjanosti

Ovaj dokument je namijenjen zaposlenicima poduzeća koji su uključeni u postupak odabira ASP ili upravljanje odnosa sa ASP kao i ASP-ima koji su u postupku izbora ili su već odabrani kao pružatelji usluga za poduzeće <>.

3.0 Oblikovanje odgovora na postavljena pitanja

InfoSec očekuje da odgovori na pitanja budu detaljni i tehničke prirode. ASP upisuje odgovore na pitanja neposredno iza pitanja na koje se odgovor odnosi. U slučaju da ASP posjeduje tehničku dokumentaciju, propise ili druge dokumente prilaže ih ispunjenom upitniku.

Odgovori na pitanja moraju biti detaljni i ne smiju biti poopćeni.

Primjer:

Neprijmjereno: "Naši poslužitelji su osigurani od napada."

Primjereno: "Na naše poslužitelje redovito instaliramo sve sigurnosne dodatke. Jedna od dužnosti našeg sistem administratora jest praćenje objava otkrivenih ranjivosti koje utječu na naše sistemsko okruženje. Politika našeg poduzeća jest da se popravci za uklanjanje ranjivosti provode u vrijeme redovitog tjednog održavanja sustava (primjerice, subotama oko 23:00h). Kritični popravci izvode se 24 sata od dostupnosti sigurnosnog dodatka. Potpun popis dodataka koji su instalirani na našim poslužiteljima poduzeće <> može dobiti na uvid.«

Neprihvatljivo: "Koristimo šifriranje."

Prihvatljivo: "Sva komunikacija među lokacijom poduzeća i lokacijom naručitelja bit će osigurana IPSec ESP *tunnelingom* i korištenjem 168-bitne TripleDES enkripcije i SHA-1 autentifikacije. Sve izmjene ključeva za enkripciju i autentifikaciju odvijaju se razdvojenim komunikacijskim putevima upotrebom infrastrukture javnog ključa (PKI).«

4.0 Standardi

4.1 Opća sigurnost

1. Sa svrhom osiguranja usklađenosti sa standardima poduzeće <> pridržava pravo na periodične preglede infrastrukture ASP-a. Poduzeće <> može izvoditi bezopasne preglede, primjerice *port scanning*, bez prethodne najave. Poduzeće <> može izvesti temeljitije preglede, penetracijske testove i fizičke preglede prethodno se najavivši 24 sata prije izvođenja testa.
2. ASP mora predložiti dokumentaciju iz koje je vidljiva predložena arhitektura za programsko okruženje poduzeća <>. Dokumentacija mora sadržavati objašnjenje veza programskog okruženja poduzeća <> i ostalih susjednih mrežnih okruženja, potpun dijagram toka, opis pohrane podataka poduzeća, opis aplikacije koja obrađuje podatke te opis postavljenih sigurnosnih mehanizama.
3. U slučaju otkrivanja sigurnosnog propusta ASP mora biti sposoban odmah onemogućiti cjelokupan sustav ili isključiti kritičnu komponentu sustava.

4.2 Fizička sigurnost

1. Oprema na kojoj gostuje aplikacija poduzeća <> fizički se mora nalaziti na osiguranom prostoru do kojeg pristup imaju samo ovlaštene osobe koje se identificiraju službenom karticom.
2. Oprema ASP infrastrukture (poslužitelji, mrežna oprema, ...) mora biti smještena u zaključane systemske ormare.
3. Poduzeće <> ima glavni utjecaj pri odlučivanju kojoj osobi je dozvoljeno stupiti u prostor u kojem se nalazi oprema za potrebe poduzeća te tko ima pravo pristupa opremi u kojoj se nalazi aplikacija poduzeća <>.
4. ASP mora obavijestiti poduzeće <> koji će od njegovih zaposlenika imati pristup sistemskom okruženju za potrebe poduzeća <>.
5. ASP mora upoznati odgovarajuće strukture poduzeća <> s postupcima koje provodi za provjeravanje svojih zaposlenih i s rezultatima tih postupaka prije nego što InfoSec izradi dozvolu za korištenju djelatnosti ASP.

4.3 Osiguranje mreže

1. Segment mreže na kojem se nalazi aplikacija za potrebe poduzeća <> mora biti potpuno odvojen od segmenata mreže namjenjenih ostalim korisnicima djelatnosti ASP. Pri tome se misli da ASP mora osigurati zasebne poslužitelje i ostalu infrastrukturu.
2. Kako će biti uređen protok podataka između poduzeća <> i ASP? Pozornost moramo posvetiti sljedećem:
 - a. Ako će poduzeće <> biti povezano s ASP preko posebne veze (npr. zakupljen vod, Frame Relay), ona mora biti zatvorena u ekstranet segmentu mreže poduzeća <>. Nadzor i upravljanje veze preuzet će skupina za nadzor i upravljanje komunikacijskim povezivanjem s partnerima.
 - b. Ako će se razmjena podataka između poduzeća <> i ASP odvijati putem javnih mreža kao što je Internet, ASP mora osigurati požarne pregrade s odgovarajućom tehnologijom, dok tijek podataka mora biti zaštićen odgovarajućim kriptografskim metodama.

4.4 Zaštita poslužitelja

1. ASP mora otkriti na koji su način poslužitelji zaštićeni od napada na kojima će se nalaziti aplikacija za potrebe poduzeća <>. ASP može priložiti raspoloživu dokumentaciju u vezi s intervencijom u povećanju sigurnosti poslužitelja.
2. ASP mora predložiti popis svih instaliranih zakrpi operacijskog sustava, poslužiteljske aplikacije, baza podataka i ostalih važnih aplikacija.
3. ASP mora predočiti način i vremenske okvire instaliranja sigurnosnih popravaka. Kako ASP brine za praćenje otkrivanja ranjivosti i kakva je njegova politika instalacije sigurnosnih popravaka?
4. ASP mora otkriti postupke za nadzor integriteta i raspoloživosti poslužitelja.
5. ASP mora izraditi politiku upravljanja zaporkama za pristup opremi za potrebe poduzeća <>. Politika mora sadržavati odredbe o: najmanjem broju znakova u zaporkama, načine njihovog generiranja i vremenske okvire njihovih valjanosti.
6. Razumljivo je da poduzeće ne može otkriti interna korisnička imena i zaporke trećim stranama. Poštujući to ograničenje ASP predlaže načine za autentifikaciju korisnika.
7. ASP mora posredovati informaciju o postupcima kreiranja, upravljanja i ukidanja sistemskih, administrativnih i korisničkih računa. Informacija mora sadržavati opise postupaka kreiranja računa, posredovanja informacija o računu korisniku i ukidanja računa ako više nije potreban.

4.5 Zaštita mrežnih poslužitelja

1. Poduzeće može zahtjevati otkrivanje podešavanja mrežnih ili njima podupiraćih poslužitelja (pretraživači, baze podataka).
2. ASP mora poduzeću otkriti jesu li i gdje u aplikaciji ili na mrežnoj stranici upotrebljeni Java, Javascript, ActiveX, PHP, ASP ili slične tehnologije.
3. U kojem je programskom jeziku napisana pozadinska aplikacija (C, Perl, Python, VBScript itd.)?
4. Na koji način ASP garantira kakvoću sigurnosnih mehanizama ugrađenih u aplikaciju? Kako se provjerava djelovanje autentifikacije, autorizacije i obračuna kao i u svim drugim aktivnostima u okviru sigurnosne arhitekture?
5. Da li ASP izvodi pregled programskog koda, uključujući CGI, Java i slične, sa svrhom otkrivanja ranjivosti? Tko izvodi takve preglede, kakvi su njihovi rezultati te kakve su mjere za uklanjanje ranjivosti? Ako se pregled programskog kôda ne izvodi, ASP može iznijeti vlastiti pogled na tu problematiku.

4.6 Šifriranje podataka

1. Na infrastrukturi poduzeća <> ne smiju se koristiti kriptografske metode koje su rezultat vlastitog razvoja. Bilo koji simetrični ili asimetrični algoritam koji se koristi u infrastrukturi poduzeća <> mora sadržavati algoritme koji su bili objavljeni i ocijenjeni od strane kriptografske zajednice.
2. Korišteni enkripcijski algoritmi moraju biti usporedivi s 168-bitnim 3DES.
3. Preporučene funkcije su SHA-1 i MD-5.
4. Protok podataka između poduzeća i ASP javnom mrežom mora biti osiguran jednom od slijedećih kriptografskih tehnologija: IPSec, SSL, SSH/SCP, PGP.
5. Ako aplikacija za potrebe poduzeća <> zahtjeva PKI, o tome je potrebno obavjestiti InfoSec poduzeća kako bi se dobile dodatne upute.