POSLOVNI RIZIK & KRIZNI MANADŽMENT

KORPORATIVNA BEZBEDNOST & ODRŽIVI RAZVOJ

SEEI Institut – Visoke performanse – Niži troškovi

Tradicionalni pristupi korporativnoj bezbednosti više nisu dovoljni.

www.see-institute.org

Sadržaj

Na poslednjoj konferenciji posvećenoj digitalnom ratu u svetu, direktori Nacionalnih bezbednosnih agencija, izrazili su zaključak da je digitalni rat postao najveća opasnost preduzećima širom sveta.

"Ono što se dešava u poslednjih nekoliko godina u digitalnim mrežama.....je najveća krađa koju smo videli u istoriji. Gubici intelektualne svojine su zapanjujući. Problem je dostigao te razmere da stvara negativne efekti svim industrijama i svakom sektoru privrede i Vlade, i zato ga svakako moramo izbaciti u prvi plan."

UVOD

Korporativna bezbednost zahteva urgentnu pažnju kompanija

DEO 1

U poslednjih pet godina, pretnje digitalnoj imovini preduzeća su značajno porasle – u broju, obimu i sofisticiranosti. Posebno je u porastu broj malicioznih napada od strane eksternih subjekata. U 2008, samo **12%** zloupotreba ili krađe podataka je bio posledica napada od strane eksternih subjekata. Broj napada je porastao na **24%** u 2009 i **31%** u 2010. Samo neki od skorašnjih događaja – najbolje ilustruju opseg problema sa kojim se kompanije širom sveta suočavaju.

Na primer, Sony je pretrpeo masivnu zloupotrebu svoje mreže korisnika za online video igrice koja je imala za posledicu krađu ličnih podataka, uključujući informacije o kreditnim i debitnim karticama više od 100 miliona korisnika njihovih usluga. Ovo je mogla biti, u stvari, jedna od najskupljih zloupotreba u istoriji: stručnjaci procenjuju da je napad mogao koštati kompaniju Sony i emitente kreditnih kartica između **$ 1 i $ 2** milijardi.

Možda je još podmukliji napad na email bazu kompanije Epsilon, koja je sadržala lične informacije potrošača. Kompanija je u svojoj bazi imala podatke 2.500 kompanija za koje je Epsilon pružao usluge digitalnih marketing kampanja. Ovaj pokušaj, bi omogućio hakerima da konstantno sprovode mahinacije nad milionima korisnika ovih poznatih brendova.

Čak i više štete kompanijama nanose napadi na njihovu intelektualnu svojinu (IP) i druge poverljive informacije koje, ako su ukradene, mogu da ugroze konkurentske pozicioniranje kompanije i održivosti na svojim izabranim tržištima. Prema nekim procenama, vrednost korporativnih i vladinih informacija koje su ukradene ili izgubljene iznosi oko **$ 1** trilion. Jedna kompanija je izgubila tehnologije vredne $ 1 milijardu dolara, za koju joj je trebalo više od 20 godina da se razvije. Nnedavno otkriveni petogodišnji sajber napadi na širok opseg visoko- profilisanih kompanija širom industrije, što je rezultiralo krađom vredne intelektualne svojine, služio je kao upozorenje drugim preduzećima.

Eksterni subjekti nisu jedina pretnja kompanijama o kojima moraju brinuti. Zloupotrebe su u najvećoj meri posledica - slučajne ili namerne - greške u sistemu, ili zaposlenih. Vikiliks je do sada dobro - poznat primer takvog "Inside Job".

Međutim, i drugi slučajevi nepoštovanja sistema bezbednosti su takođe česti, kao što su krađe i prodaja informacija zaposlenih konkurentima, ili skidanje i uzimanje osetljivih podataka otpuštenih radnika novim poslodavcima, ostavljanje neobezbeđenog laptopa na javnom mestu, uvođenje malverzacija ili virusa u korporativni sistem itd ...

Usled složenosti savremenog poslovanja pristup SEEI –a korporativnoj bezbednosti se razlikuje, jer u našem fokusu pored svih gore navedenih informativnih rizika, analiziramo i ostale rizike i pretnje koje mogu direktno da utiču na ekonomsku održivost preduzeća, poput energetskog rizika, pravnog, finansijskog itd. Samo sveobuhvatnim pristupom rizicima koji mogu da utiču na materijalnu i nematerijalnu aktivu kompanije u određenoj industriji, možemo poslovanje zaista učiniti sigurnim.

U našem pristupu idemo čak i dalje, i koristimo naše znanje i iskustvo u energetskoj efikasnosti za kontinuirano finansiranje razvoja korporativne bezbednosti unutar kompanije, ostvarenim uštedama energije.

Dugoročno održivi razvoj kompanije je uvek u našem fokusu.

Korporativna bezbednost zahteva urgentnu pažnju kompanija

Tabela 1: Učestalost kojom kompanije obnavljaju svoju strategiju korporativne bezbednosti

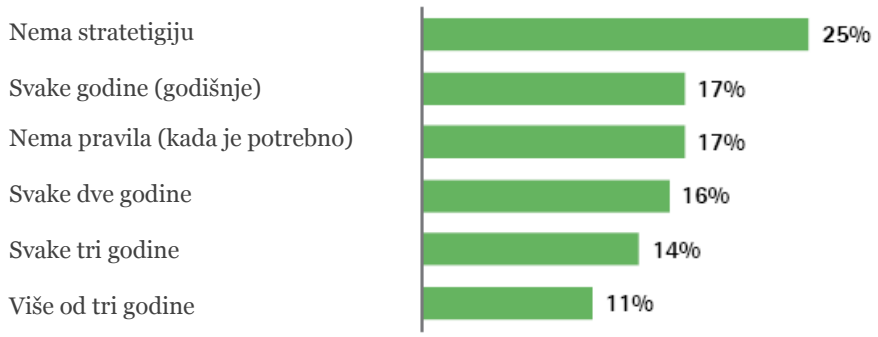


Tabela 2: Opseg u kome su ciljevi korporativne bezbednosti integrisani sa IT aktivnostima

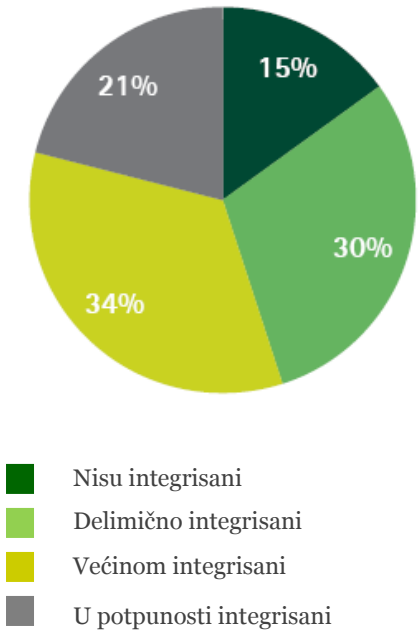
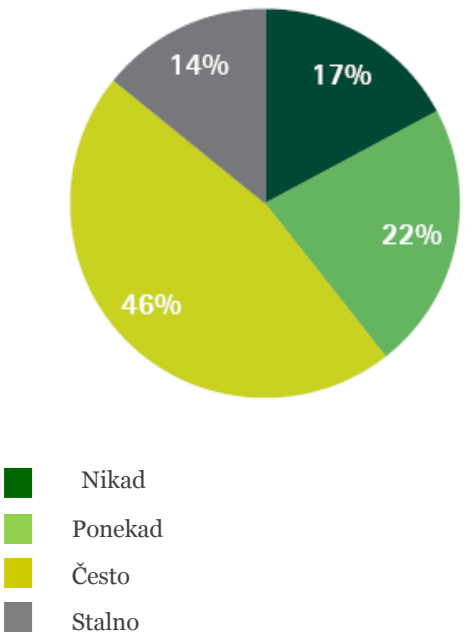


Tabela 3: Opseg u kome ciljevi bezbednosti ometaju realizaciju ciljeva kompanije



6 principa za dostizanje visokih performansi u korporativnoj bezbednosti

Bazirano na našem iskustvu—a posebno na tome šta je opseg sektora korporativne bezbednosti danas — identifikovali smo **6** ključnih principa čijom će primenom kompanije dostići visoke performance u korporativnoj bezbednosti.

6 SEEI PRINCIPA ZA DOSTIZANJE VISOKIH PERFORMANSI:

1. Bezbednost se ne odnosi samo na IT , već na organizaciju kao celinu.
2. Strategija bezbednosti, mora biti u tesnoj vezi sa ciljevima i strategijom na nivou organizacije.
3. Primarni fokus sektora bezbednosti, ne sme da bude samo ispunjavanje zakonskih odredbi.
4. Efikasna bezbednost zahteva dovoljan iznos finansijskih sredstava.
5. Najbolja odbrana je dobar napad.
6. Glavni fokus korporativne bezbednosti nije IT bezbednost, već ekonomska održivost preduzeća, i svi faktori koji je mogu ugroziti.

Statistika

DEO 2

Pretnje po informativnu bezbednost kompanija

Preduzeća se danas suočavaju sa širokim spektrom bezbednosnih pretnji a koje su dovele do stvarne povrede u ogromnoj većini kompanija. RazvojIT inovacija je pomogao da se poveća učestalost takvih pretnji.

Tabela 4: Najozbiljnije pretnje po IT bezbednost kompanija

Tabela 5: IT inovacije viđene kao pretnja po bezbednost informacija

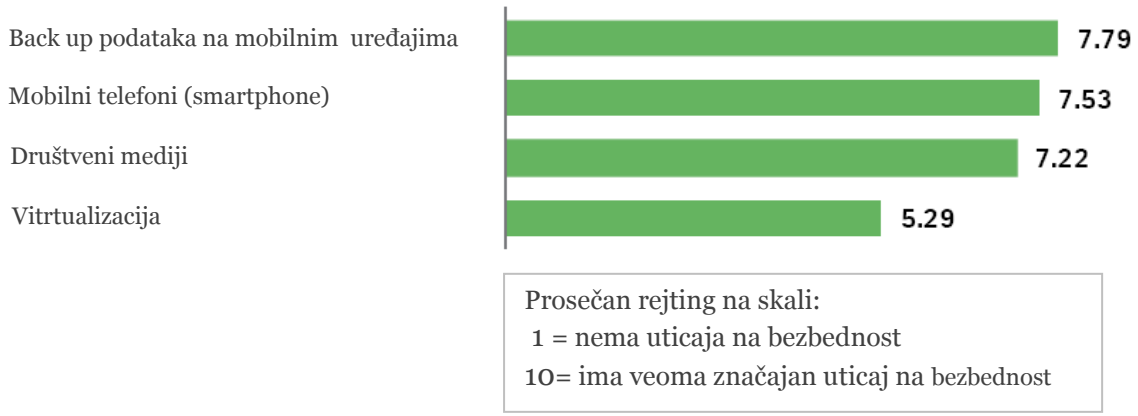


Tabela 6: Prepreke za kompanije da preuzmu mere za uanpređenje korporativne bezbednosti

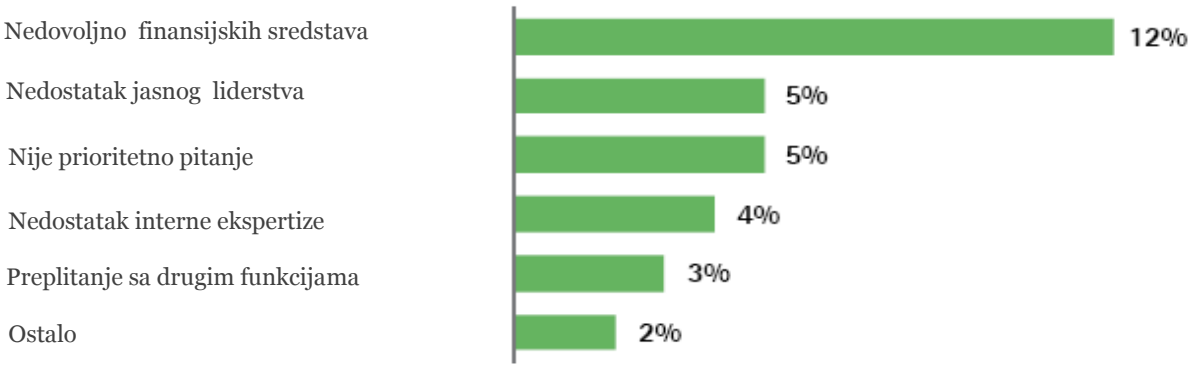


Tabela 7: Načini na koji kompanije mere efikasnost sektora bezbednosti

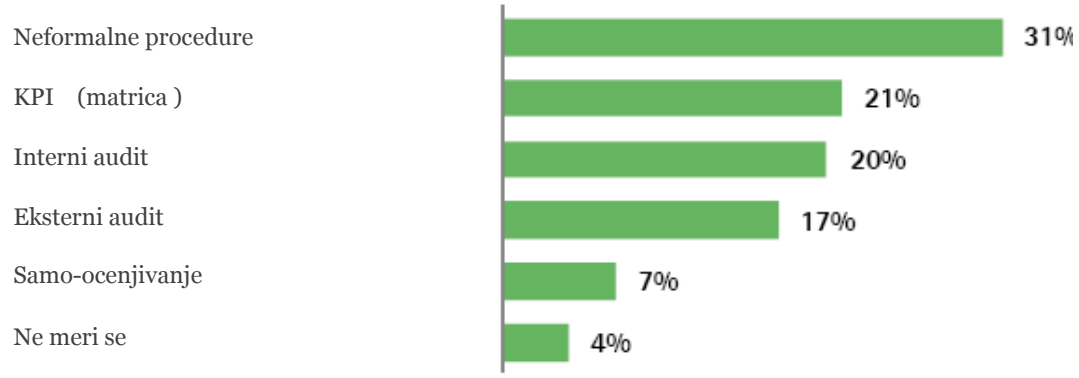
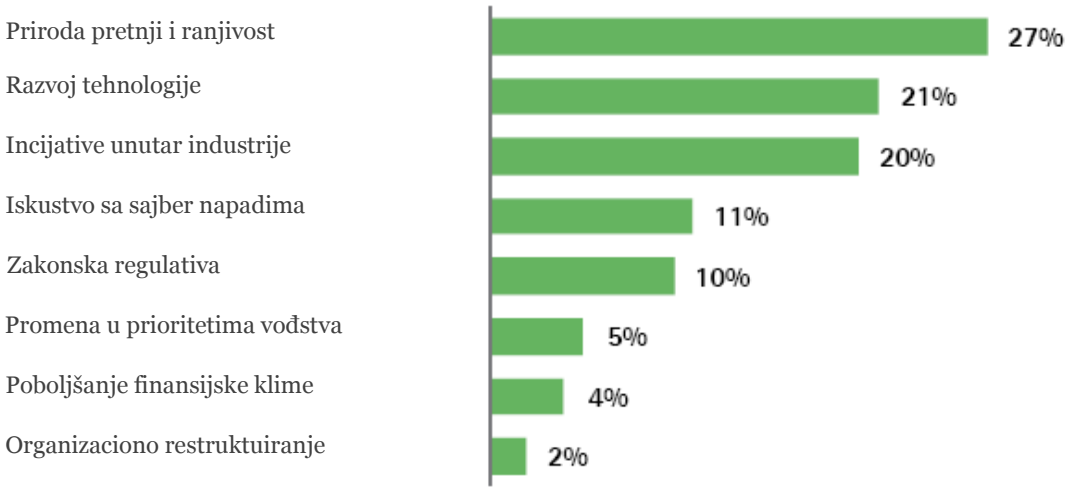


Tabela 8: Načini na koji kompanije definišu svoj nivo izloženosti riziku

Tabela 9: Faktori koji vode kompanije da se razvijaju ka korporativno bezbednoj kompaniji



SEEI metodologija za razvoj korporativne bezbednosti

DEO 3

10 SEEI - koraka za razvoj korporativne bezbednosti kompanija

Na osnovu naše dosadašnje prakse — definisali smo **10** ključnih koraka koji će pomoći kompanijama da ostvare visoke performanse u korporativnoj bezbednosti.

10 SEEI KORAKA ZA RAZVOJ KORPORATIVNE BEZBEDNOSTI:

1. Strategija korporativne bezbednosti
2. Definisanje korporativne politike
3. Razvoj bezbednosne kulture
4. Procena rizika
5. Razvoj sistema za klasifikaciju dokumenata
6. IT bezbednost & tehnologije
7. Krizni menadžment
8. Odgovor na incidente
9. Lična bezbednost
10. Fizička bezbednost

O nama:

SEEI Institut je osnovan 2010 godine sa ciljem da u saradnji sa istaknutim stručnjacima razvija dugoročne strategije, politike, planove i programe i realizuje obuku neophodnih kadrova za unapređenje energetske efikasnosti i korporativne bezbednosti, saglasno praksi razvijenih zemalja, i na taj način da i svoj lični doprinos razvoju privrede Republike Srbije i regiona.

SEEI Institut se bavi kontinurianom analizom tržišta, inovacija i tehnologija koje su dizajnirane za rešavanje najvećih svetskih izazova danas, kao što su energetska efikasnost i korporativna bezbednost, a sa ciljem da kontinuraino doprinesi ekonomskoj održivosti preduzeća i ekonomije.

Preko **50** realizovanih međunarodnih projekata, na području energetske efikasnosti i korporativne bezbednosti kako u zemlji, tako i u inostrastvu, **25 godina** međunarodnog iskustva i razvijena **mreža** domaćih i inostranih stručnjaka na području energetske efikasnosti i korporativne bezbednosti, govore u prilog našoj nedvosmislenoj fokusiranosti na performanse, kvalitet, i isporuku vrednosti u svemu što radimo.

SOUTHEAST EUROPEAN INSTITUTE

Kronštatska br.5

11000 Belgrade

T: + 381 11 26 41 055

E: office@see-institute.org

W: www.see-institute.org