Objava

Datum	**23. listopada 2017.**
Kontakt	Jasna Kržanić, Marketing i komunikacije, PwC hrvatska Tel.: +385 98 383 012 Email: jasna.krzanic@pwc.com
Broj stranica	3

Organizacije se ne uspijevaju uspješno pripremiti za kibernetičke napade, kažu u PwC-u

Za uspjeh su ključni predanost vodstva, otpornost i suradnja

- Četrdeset posto ispitanika u istraživanju navodi prekid operacija kao najveću posljedicu kibernetičkog napada, nakon čega slijedi kompromitiranje osjetljivih podataka (39 %), šteta za kvalitetu proizvoda (32 %) i šteta za ljudski život (22 %).
- Četrdeset i četiri posto od 9.500 ispitanih rukovoditelja iz 122 zemlje kaže da nema cjelovitu strategiju informacijske sigurnosti.
- Četrdeset i osam posto nema program edukacije zaposlenika za osviještenost o sigurnosti, a 54 % nema proces za odgovaranje na incidente.
- Kad dođe do kibernetičkih napada, većina kompanija žrtava kaže da ne mogu jasno odrediti krivce. Samo 39 % ispitanika u istraživanju kaže da je vrlo sigurno u svoje sposobnosti utvrđivanja odgovornosti.

Izuzetno velike povrede kibernetičke sigurnosti postale su gotovo uobičajene te redovito pune naslovnice koje upozoravaju korisnike i rukovoditelje. No, unatoč svoj pažnji koju su takvi incidenti privukli proteklih godina, mnoge organizacije širom svijeta još se uvijek bore da shvate i počnu upravljati sve većim kibernetičkim rizicima u sve složenijem digitalnom društvu.

PwC objavio svoje istraživanje o Globalnom stanju informacijske sigurnosti za 2018. godinu (*2018 Global State of Information Security*® - GSISS), na temelju odgovora više od 9.500 rukovoditelja poslovanja i tehnologije iz 122 zemlje.

Rukovoditelji širom svijeta prepoznaju sve veću opasnost od kibernetičke nesigurnosti. Četrdeset posto ispitanika u istraživanju navodi prekid operacija kao najveću posljedicu kibernetičkog napada, 39 % navodi kompromitiranje osjetljivih podataka, 32 % navodi štetu za kvalitetu proizvoda, a 22 % navodi štetu za ljudski život.

Ipak, unatoč ovoj osviještenosti, mnoge tvrtke izložene riziku od kibernetičkih napada i dalje su nespremne da se s njima nose. Četrdeset i četiri posto ispitanika kaže da nema cjelovitu strategiju informacijske sigurnosti. Četrdeset i osam posto kaže da nema program edukacije zaposlenika za osviještenost o sigurnosti, a 54 % kaže da nema postupak za odgovaranje na incidente.

Kako kibernetička međuovisnost utječe na globalni rizik

Studije slučajeva nekibernetičkih katastrofa pokazale su da kaskadni događaji obično započnu nestankom električne energije — mnogi sustavi pogođeni su odmah ili u roku od jednog dana, što znači da općenito ima malo dragocjenog vremena za rješavanje inicijalnog problema prije no što se kaskadno proširi. Međuovisnosti između vitalnih i nevitalnih mreža često prolaze neopaženo dok se ne dogodi katastrofa. Mnogi ljudi širom svijeta, naročito u Japanu, Sjedinjenim Američkim Državama, Njemačkoj, Ujedinjenom Kraljevstvu i Južnoj Koreji, zabrinuti su zbog mogućih kibernetičkih napada iz drugih zemalja. Alati za provođenje kibernetičkih napada množe se diljem svijeta. Manje nacije nastoje razviti sposobnosti poput onih koje koriste veće zemlje. A curenje alata za hakiranje iz

američke Agencije za nacionalnu sigurnost (NSA) učinilo je visoko sofisticirane alate dostupnima zlonamjernim hakerima.

Kad dođe do kibernetičkih napada, većina kompanija žrtava kaže da ne mogu jasno odrediti krivce. Samo 39 % ispitanika u istraživanju kaže da je vrlo sigurno u svoje sposobnosti utvrđivanja odgovornosti.

Rastuća proizvodnja nesigurnih uređaja za Internet stvari (*internet-of-things*) čini da su slabe točke kibernetičke sigurnosti široko rasprostranjene. Sve veće prijetnje integritetu podataka mogle bi potkopati pouzdane sustave i uzrokovati fizičku štetu oštećivanjem vitalne infrastrukture.

Istovremeno, postoji veliki nesrazmjer u pripravnosti kibernetičke sigurnosti među državama svijeta. U našoj studiji GSISS za 2018. godinu, učestalost organizacija koje posjeduju cjelovitu strategiju kibernetičke sigurnosti naročito je visoka u Japanu (72 %), gdje se kibernetički napadi smatraju vodećom prijetnjom nacionalnoj sigurnosti, te u Maleziji (74 %).

U svibnju 2017. godine, vođe iz skupine G-7 obvezali su se surađivati međusobno i s drugim partnerima kako bi se riješili kibernetički napadi i ublažio njihov učinak na vitalnu infrastrukturu i društvo. Dva mjeseca kasnije, vođe iz skupine G-20 ponovno su naglasili potrebu za kibernetičkom sigurnošću i povjerenjem u digitalne tehnologije. Zadatak koji im predstoji ogroman je.

Sljedeći koraci za vođe u poslovnom svijetu

Dakle, što mogu učiniti vođe u poslovnom svijetu kako bi se učinkovito pripremili za kibernetičke napade? PwC preporučuje tri ključna područja:

Članovi uprava moraju biti predvodnici, a uprave se moraju uključiti: Rukovoditelji na čelu poslovanja moraju preuzeti odgovornost za izgradnju kibernetičke otpornosti. Postavljanje strategije upravljanja kibernetičkim rizicima i rizicima privatnosti u cijelom poduzeću koja kreće od vrha prema dolje ključno je.

Težiti otpornosti kao putu prema nagradama, ne samo kako bi se izbjegao rizik: Postizanje veće otpornosti na rizik je put prema snažnijem, dugoročnom ekonomskom uspjehu.

Svrhovita suradnja i korištenje naučenih lekcija: Poslovne i političke vođe moraju surađivati i izvan organizacijskih, sektorskih i nacionalnih granica kako bi se identificirali, mapirali i testirali rizici kibernetičke ovisnosti i međuspojivosti te poboljšala otpornost i upravljanje rizicima.

„Vrlo je malo poslovnih problema koji prožimaju gotovo svaki aspekt poslovanja i trgovanja kao što je to danas kibernetička sigurnost“, rekao je David Burg, globalni voditelj usluba kibernetičke sigurnosti u PwC-u. „Javno-privatna koordinacija ključna je za učinkovitu kibernetičku sigurnost.“.

Napomene urednicima:

1. *Global State of Information Security*® za 2018. godinu je globalna studija o stanju informacijske sigurnosti koju su izradili PwC, *CIO* i *CSO*. Provedena je putem interneta od 24. travnja do 26. svibnja 2017. godine. Čitatelji časopisa *CIO* i *CSO* te klijenti PwC-a iz 122 zemlje bili su pozvani putem e-maila na sudjelovanje u istraživanju.
2. Rezultati navedeni u ovom izvješću temelje se na odgovorima više od 9.500 poslovnih i IT direktora, uključujući generalne direktore (CEO), direktore financija (CFO), direktore informacijske sigurnosti (CISO), direktore za informacije (CIO), direktore za sigurnost (CSO), potpredsjednike te direktore zadužene za IT i informacijsku sigurnost iz 122 zemlje. 38 % ispitanika bilo je iz Sjeverne Amerike, 29 % iz Europe, 18 % iz Azije i Pacifika, 14 % iz Južne Amerike, a 1 % s Bliskog Istoka i iz Afrike.

3. Ispitan je niz javnih i privatnih organizacija: 28 % ispitanika bilo je iz malih poduzeća s godišnjim prihodima manjima od 100 milijuna dolara, 46 % ispitanika bilo je iz organizacija s prihodima višim od 500 milijuna dolara, a 4 % su bile neprofitna, vladina ili obrazovna tijela.
4. Izvješće možete preuzeti na: http://www.pwc.com/us/en/cybersecurity/information-security-survey.html

O CIO-u
CIO se usredotočuje na privlačenje visoke koncentracije CIO-a i direktora poslovnih tehnologija s najboljim uvidom kolega iste razine i stručnim znanjem o poslovnoj strategiji, inovacijama te vodstvu. Kako organizacije rastu s digitalnom transformacijom, CIO svojim čitateljima nudi ključne uvide u razvoj karijere, uključujući certifikate, prakse zapošljavanja i razvoj vještina. Nagrađivani portfelj CIO-a - CIO.com, CIO programi za rukovoditelje, CIO usluge strateškog marketinga, CIO forum na mreži LinkedIn, Odbor direktora CIO-a te primarno istraživanje CIO-a - pruža tehnološki voditeljima analizu i uvid u trendove u informacijskim tehnologijama te duboko razumijevanje uloge IT-a u postizanju poslovnih ciljeva. Odbor direktora CIO-a je stručna organizacija CIO-a, stvorena da predstavlja nepristranu i pouzdanu savjetodavnu skupinu iste razine. CIO izdaje tvrtka IDG Communications, Inc. Informacije o tvrtki dostupne su na www.idg.com.

O CSO-u
CSO je vrhunski izvor sadržaja za donositelje odluka vezanih za sigurnost koji vode poslove „upravljanja poslovnim rizicima“ u svojim organizacijama. Već više od 15 godina, CSO-ova nagrađivana internetska stranica (CSOonline.com), konferencije za direktore, rješenja za strateški marketing i istraživanja pomogli su donositeljima odluka vezanih za sigurnost u rješavanju IT i korporativnog/fizičkog rizika u svojim organizacijama i omogućili dobavljačima na području sigurnosti da dopru do ove publike. Na temelju uredničkih tema i dizajna, nagrada Folio Eddie proglasila je CSOonline.com najboljom internetskom stranicom za B2B tehnologije u 2015. i 2016. godini. Kako bi pomogli CSO-ima u edukaciji zaposlenika svojih organizacija o korporativnim i osobnim sigurnosnim praksama, CSO izdaje i tromjesečni bilten *Security Smart*. CSO izdaje tvrtka IDG Communications, Inc. Informacije o tvrtki dostupne su na www.idg.com.

O PwC-u
Cilj PwC-a je izgraditi povjerenje u društvo i riješiti važne probleme. Mreža smo tvrtki u 158 zemalja s više od 236.000 zaposlenika koji zalažu za pružanje kvalitetnih usluga na područjima revizije i računovodstvenog savjetovanja, poslovnog savjetovanja i poreznih usluga. Posjetite www.pwc.hr da biste doznali više i rekli nam što vam je važno.

PwC se odnosi na mrežu PwC-a i/ili jednu ili više tvrtki članica, od kojih je svaka zasebna pravna osoba. Za više detalja posjetite www.pwc.com/structure.