STANJE INFORMACIJSKE SIGURNOSTI 2020

diverto

Diverto d.o.o., jedno od vodećih društava na području primjene informacijske sigurnosti, donosi osvrt na stanje informacijske sigurnosti u Hrvatskoj.

Osvrt i preporuke donose se kroz tri različite, ali međusobno povezane perspektive informacijske sigurnosti korištenjem top-down pristupa: upravljačke (governance), napadačke (offensive) i obrambene (defensive) perspektive.

Osvrt temeljimo na:

- procjenama stanja informacijske sigurnosti u organizacijama javnog i privatnog sektora u našoj zemlji
- podacima prikupljenima iz aktivnosti Diverto Sigurnosnog operativnog centra
- rezultatima provjere ranjivosti i penetracijskih testiranja

Sadržaj

COVID-19 pokazao nam je koliko možemo biti slijepi ukoliko redovno ne testiramo ili pak nemamo tehničkih ili ljudskih mogućnosti prepoznati incident. Također, pokazao nam je koliko brzo i eksponencijalno problem može narasti ako ne reagiramo na vrijeme.

- Vlatko Košturjak,

CTO

01

UPRAVLJAČKA PERSPEKTIVA

Ključni pokazatelji u promatranom periodu

- Izraženo korištenje socijalnog inženjeringa kao vektora napada
- Povećana aktivnost napadača na ciljeve u različitim industrijama
- Nedostatak planiranja kapaciteta rada za vrijeme izvanredne situacije
- Nemogućnost pravovremenog odgovora na izvanredne situacije zbog nepostojećih ili neažuriranih planova kontinuiteta poslovanja

Procjena kretanja u 2020.

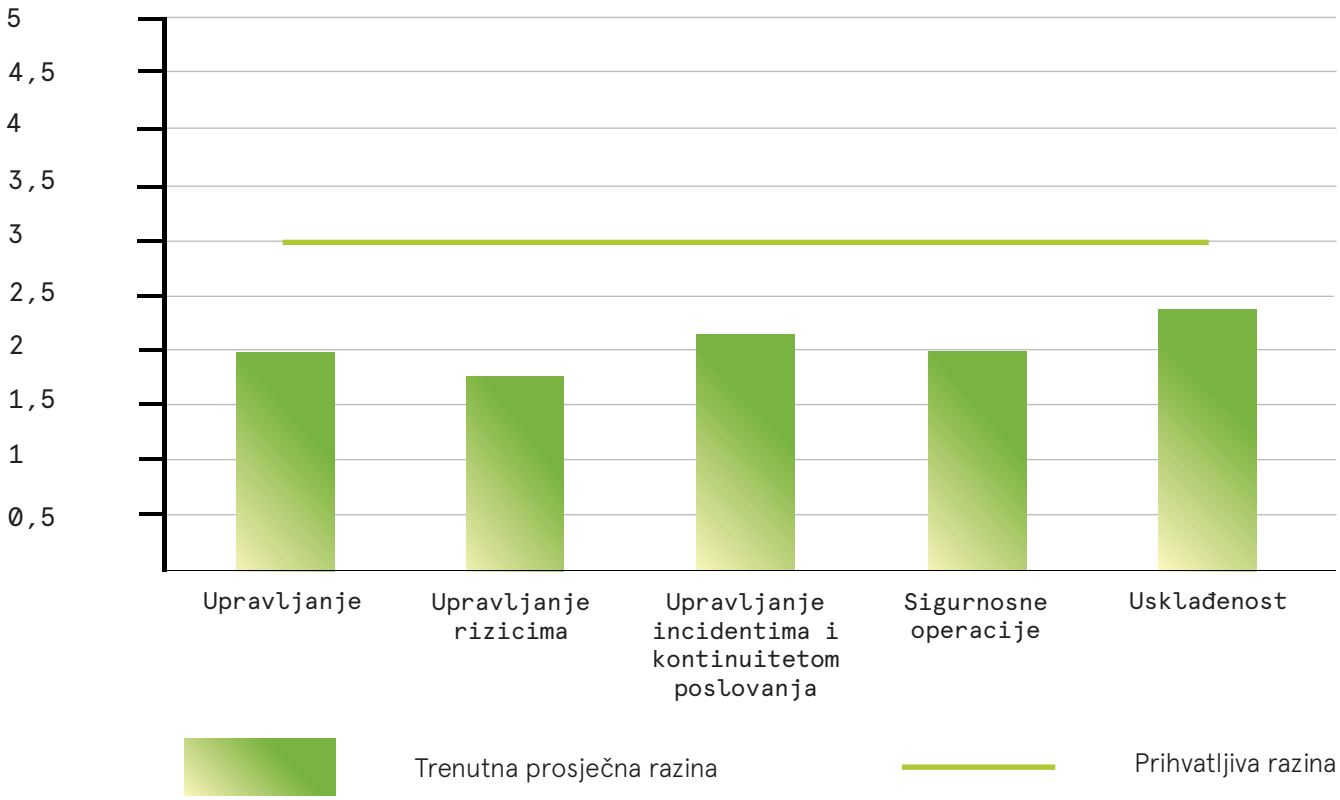
- Oporavak poslovanja nakon pandemije virusa COVID-19
- Naglasak na radu „od doma"
- Promjena percepcije važnosti planiranja kontinuiteta poslovanja
- Optimizacija poslovnih procesa kroz digitalizaciju
- Nastavak ulaganja u informacijsku sigurnost
- Podizanje svijesti o odgovornosti organizacija za čuvanje podataka na cloud rješenjima

Pozitivni pomaci

- Implementacija NIS direktive u nacionalno zakonodavstvo omogućuje reguliranje dosad nereguliranih sektora
- Povećano korištenje EU fondova za razvoj upravljačkih sustava (ISO i slične norme)
- Povećanje ulaganja u osvješćivanje i educiranje zaposlenika

Iako su u Hrvatskoj vidljivi pozitivni pomaci, i dalje postoji nedostatak razumijevanja uloge informacijske sigurnosti, kao i njezine implementacije unutar organizacija. Pravila dobre prakse najviše se prate u reguliranim sektorima, kao što su financijski i telekomunikacijski sektor. I dalje postoji ovisnost o IT-u koju prate nejasni troškovi za sigurnost i niska razina detekcije incidenata.

Stanje informacijske sigurnosti



Najveći nedostatak organizacije pokazuju na području osviještenosti zaposlenika i sigurnosnih operacija, odnosno na području dnevnog upravljanja sigurnošću organizacija i upravljanja rizicima. I dalje samo manji broj organizacija sigurnosne mjere bazira na analizi rizika.

Stanje organizacija u Hrvatskoj*

1. FILOZOFIJA LJUDI

- Sigurnost nije prepoznata na svim razinama
- Sigurnost je često dio IT-a
- Visoka ovisnost o pojedincima

2. PROCESI

- Procesi djelomično formalizirani
- Rijetko potpuno predvidivi
- Ne integriraju više poslovnih funkcija

3. TEHNOLOGIJA

- Mehanizmi zaštite nisu centralizirani
- Korištenje automatiziranih rješenja bez prikladne implementacije i obuke osoblja
- Detekcija incidenata kibernetičke sigurnosti niska

* temeljeno na provjerama stanja sigurnosti u 6 mjeseci

02

DEFENZIVNA PERSPEKTIVA

Pozitivni pomaci

- Sve više organizacija odlučuje se na cjeloviti pristup informacijskoj sigurnosti kroz uvođenje SOC-a, umjesto dosadašnjeg ulaganja u SIEM sustave, čime se unaprjeđuje sigurnost aktivnim praćenjem sigurnosnih događaja. Uglavnom se radi o naprednim organizacijama koje su visoko podigle razinu informacijske sigurnosti.
- Manje organizacije, često pritisnute negativnim iskustvima, odlučuju se na vanjsku potporu kroz usluge dediciranog tima za odgovor na incidente s definiranim vremenom odgovora.
- U energetskom sektoru, kao i u djelatnosti proizvodnje, shvaća se važnost uvođenja SOC-a kao holističkog rješenja koje povezuje IT/OT/IoT.
- Dio organizacija primjenjuje i dobre prakse aktivnog praćenja sigurnosnih događaja, za razliku od dosadašnjeg reaktivnog pristupa.

Najčešće istrage prema MITRE Att&ck taktikama*

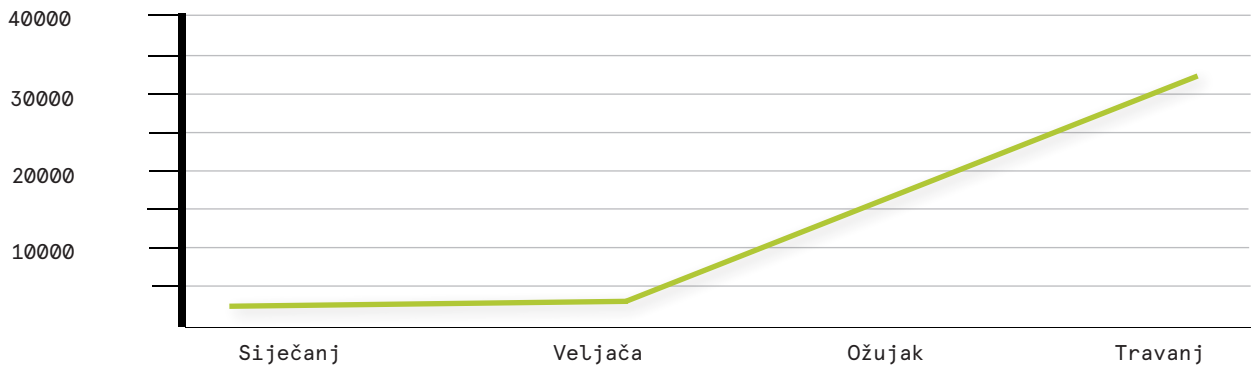
1. Credential access
2. Initial access
3. Defense evasion
4. Lateral movement
5. Execution

Rad od kuće

Osnovni izazovi koje je potrebno adresirati za vrijeme povećanog rada od kuće:

- provođenje edukacija zaposlenika o sigurnom radu od kuće
- osiguranje udaljenog pristupa velikom broju zaposlenika
- osiguranje radnih sredstava zaposlenicima za rad od kuće
- postizanje prihvatljive/podnošljive razine informacijske sigurnosti

Broj udaljenih spajanja*



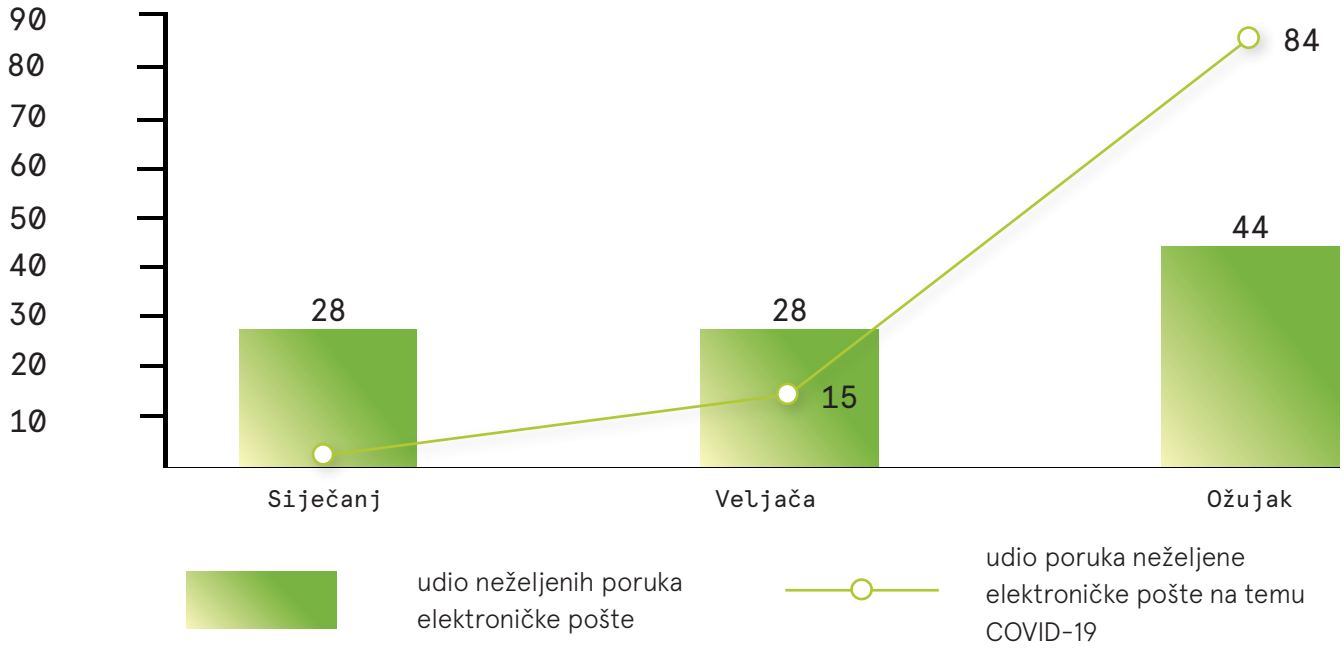
*bazirano na 5000 obrađenih alarma i 700 obrađenih istraga Diverto SOC tima u posljednjih 6 mjeseci

Phishing

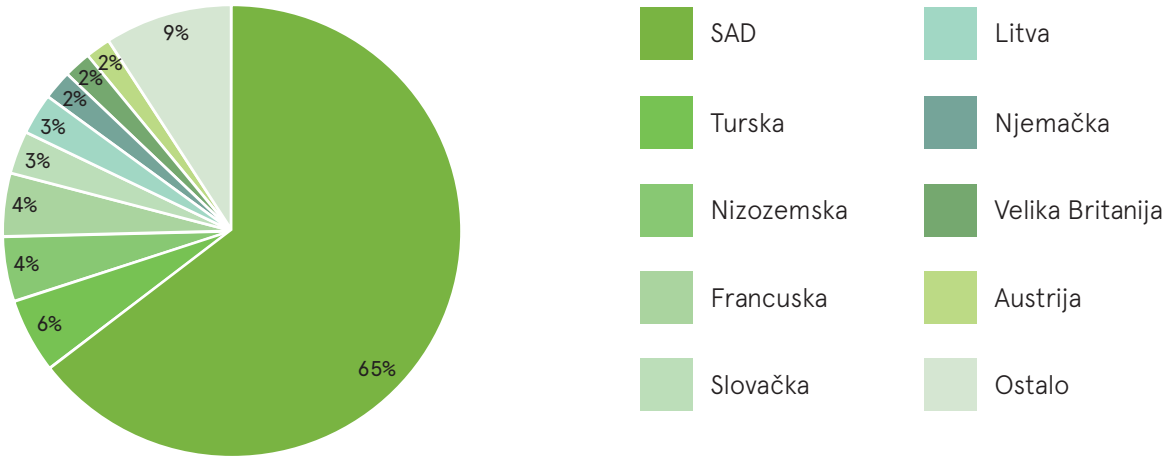
Dva su najčešća vektora ulaska zlonamjernog koda u organizaciju: putem elektroničke pošte ili kompromitirane mrežne stranice.

Trend pokušaja ulaska putem phishing poruka je u porastu, s naglaskom na broj poruka napisanih na pravilnom hrvatskom jeziku. Vrlo česta tema phishing poruka je COVID-19. Zanimljivo je da napadači prilikom slanja zlonamjernih poruka povremeno koriste i zastarjele arhivske formate kao što su .arj i .ace. Pretpostavka je da napadači koriste zastarjele formate jer administratori sustava zaštite često zaboravljaju na njih, pa tako jednostavnim trikom uspješno zaobilaze zaštitu.

Porast broja phishing poruka i trend zlouporabe pojma COVID-19 (%)*



Odakle dolaze COVID-19 zlonamjerne poruke?*



*bazirano na 5000 obrađenih alarma i 700 obrađenih istraga Diverto SOC tima u posljednjih 6 mjeseci

Iznošenjem računala izvan standardne okoline rada gubi se kontrola događaja na krajnjim radnim stanicama, čime se posao nadzora informacijske sigurnosti iznimno otežava.

– Vladimir Ožura,

viši konzultant za informacijsku sigurnost

03

OFENZIVNA PERSPEKTIVA

Ključni pokazatelji u promatranom periodu

- nedostatak procedura i sustava za upravljanje zakrpama
- nedostatak sustava za upravljanje administrativnim računima
- nedostatak nadzora nad sigurnosnim događajima na infrastrukturi
- nedostatak assume breach principa
- nedostatak komponente procjene sigurnosti tijekom implementacije

Brzim razvojem aplikacija u doba pandemije virusa COVID-19 često se ignoriraju sigurnosni zahtjevi, što rezultira velikim brojem aplikacija s povećanim brojem ranjivosti. Posebno su istaknute aplikacije koje od korisnika traže unos dokumenata (upload), pri čemu se nedovoljno provjeravaju vrste unesenih datoteka.

Pozitivni pomaci

- Uočeno je povećanje provođenja provjera ranjivosti i penetracijskih testiranja, što je moguća posljedica novih regulativa, kao što su to GDPR i NIS.
- Vidljiv je i pozitivni pomak na području zaštite krajnjih točaka, kao i nadzora nad aktivnostima unutar Active Directory infrastruktura.
- Također, zabilježene su dobre prakse provođenja naprednih napadačkih vježbi, takozvanih red i purple teaming testiranja.
- Razvijatelji aplikacija sve se više odlučuju na educiranje zaposlenika vezano uz aplikacijsku sigurnost, čime podižu vrijednost svojih isporuka.
- Sve više organizacija postavlja pravila i slijedi dobre prakse provjere, odnosno testiranja rješenja trećih strana prije odluke o nabavi.

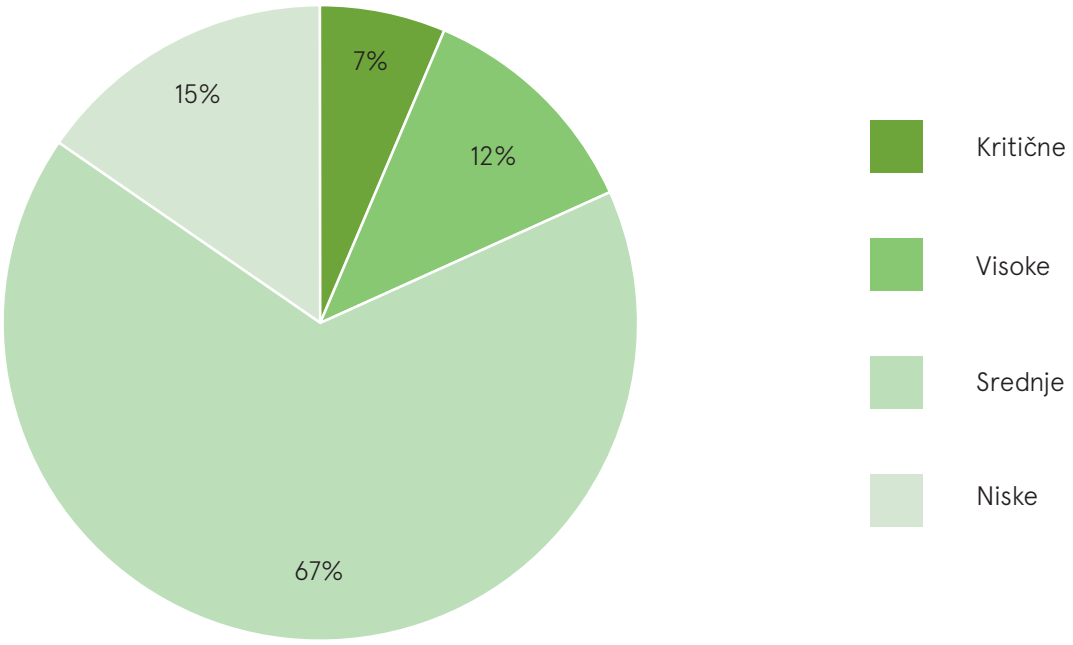
Najčešće ranjivosti na aplikacijama*

- Security misconfiguration
- Cross-site scripting
- Broken access control
- Using components with known vulnerabilities
- Injection

Najčešće ranjivosti na sustavima*

- Nedostatak zakrpa za operacijske sustave i popratni softver
- Jednostavne i inicijalno postavljene lozinke
- Korištenje istih lozinki za različite sustave
- Iskorištavanje funkcionalnosti modernih mrežnih protokola
- Korištenje protokola čistog teksta
- Nedostatak dvofaktorske autentikacije
- Nedostatak nadzora nad sigurnosnim događajima

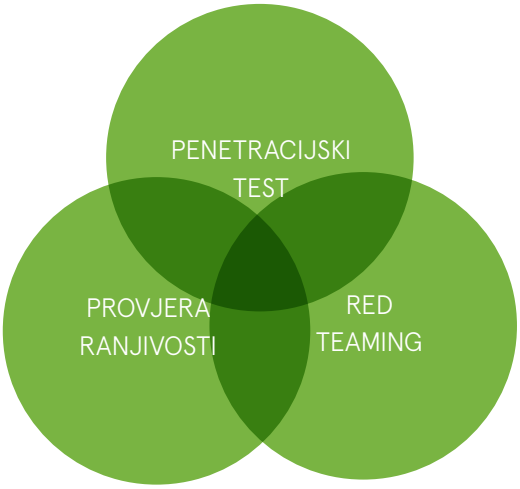
Ranjivosti prema razinama kritičnosti**



*temeljeno na ranjivostima prema OWASP za posljednjih 6 mjeseci – sumirano

**temeljeno na 47000 analiziranih ranjivosti penetracijskih testiranja u posljednjih 6 mjeseci

Razine provjere



PROVJERA RANJIVOSTI

Provjera ranjivosti je aktivnost koja pomaže da se ranjivosti identificiraju automatskim putem, a preporučeno je da se obavlja periodički. Ograničena je svojim mogućnostima, ali s druge strane, temeljna je i polazišna provjera bez koje se ne može.

PENETRACIJSKA TESTIRANJA

Korak dalje su penetracijska testiranja koja obično, osim automatske identifikacije ranjivosti, uključuju testiranje koje provode kvalificirane osobe. Ranjivosti se iskorištavaju kako bi se ostvario cilj testiranja. Prava vrijednost penetracijskog testiranja je kombiniranje ranjivosti različitih kritičnosti te njihovo iskorištavanje kako bi se pokazala ispravna kritičnost identificiranih ranjivosti. Problem je što se opseg i vrijeme testiranja vrlo često smanjuju iz različitih razloga pa spomenute prednosti ne dolaze do izražaja.

RED TEAMING

Ako želite vidjeti što napadač koji se namjeri na vašu organizaciju uistinu može napraviti te utvrditi koliko ste spremni identificirati i odgovoriti na takav napad, vrijeme je za red teaming. Jednostavno se definira cilj, a napadač se može služiti svim sredstvima kako bi došao do cilja, što uključuje iskorištavanje ranjivosti na organizacijskoj, ljudskoj i tehnološkoj razini.

ČINJENICE

Red teaming ne zamjenjuje penetracijska testiranja, niti penetracijska testiranja zamjenjuju provjeru ranjivosti. Preporuka je provoditi sve vrste testiranja.

Kvaliteta rezultata povećava se povećanjem opsega testiranja.

Kvaliteta testiranja aplikacija povećava se ukoliko se testiranje vrši uz dostupan izvorni kod. Isključivo dinamičko testiranje aplikacija smatra se zastarjelim.

Testiranje ili provjera ne bi trebala biti jedina sigurnosna kontrola koju provodite.

Prednost za napadače je što mnoge organizacije ignoriraju ranjivosti srednjeg rizika, koje se učestalo iskorištavaju (i povezuju) u svrhu provođenja uspješnog napada.

- Ivan Račić,

viši konzultant za informacijsku sigurnost

04

PREPORUKE

DIGITALIZACIJA

Proteklo razdoblje obilježila je hiperprodukcija aplikativnih rješenja, pri čemu su mnogi ignorirali potrebu analize rizika vezanih za ranjivosti takvih rješenja. To je dovelo do pojave dijela ranjivih aplikacija koje ne štite poslovne i osobne podatke na prihvatljiv način. Ponajviše se takve ranjivosti odnose na aplikacije koje zahtijevaju prijenos dokumentacije korisnika prema pružateljima usluga. Pozitivno je što su neki, prateći standardni proces rada i dobre prakse, promjenama upravljali na način koji uzima u obzir prethodno sagledavanje ranjivosti i postupke cjelovitog testiranja rješenja.

KONTINUITET POSLOVANJA

Uslijed intenzivnih seizmoloških aktivnosti na području okolice Zagreba potrebno je reevaluirati procjene utjecaja i posljedica potresa, a posebice njihovu vjerojatnost pojave. Svjedoci smo povećanja vjerojatnosti ostvarenja povezanih događaja poput požara, poplava ili urušavanja građevinskih objekata. Tradicionalna strategija odgovora na rizike potresa je djelomični prijenos rizika na treću stranu (osiguravatelja), to jest, ugovaranje polica osiguranja od požara i povezanih rizika.

Potres je, uz situaciju vezano uz pandemiju virusa COVID-19, samo podsjetnik na važnost sustavnog održavanja i testiranja realnih planova kontinuiteta poslovanja.

LJUDSKI RESURSI

Naglim prelaskom na povećani opseg rada od kuće, kao i rada u nepredvidivim situacijama, pokazalo se koliko su ljudska spremnost i svijest bitni čimbenici u održavanju prihvatljive razine informacijske sigurnosti. U organizacijama u kojima ne postoji dovoljna svijest o važnosti informacijske sigurnosti teže je provoditi potrebne mjere za vrijeme nepredviđenih ili kriznih situacija.

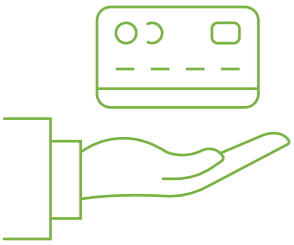
Pandemija virusa COVID-19 zasigurno je obilježila posljednje vrijeme, no razvoj sigurnih digitalnih rješenja prije i poslije ove situacije trebao bi biti imperativ svim organizacijama kako bi korisnicima pružile usluge u koje imaju povjerenja i koje će htjeti koristiti i ubuduće.

- Alen Delić,

vodeći konzultant za informacijsku sigurnost

Preporuke po sektorima

FINANCIJSKI



Reguliran i nadziran sektor kojem upravljanje rizicima nije nepoznanica. Ipak, potrebno je:

· Revidirati procjenu rizika (potres/pandemija)

· Revidirati strategiju kontinuiteta poslovanja i testirati planove oporavka

· Educirati zaposlenike o phishing napadima i posljedicama takvih napada

· Redovno provoditi testiranja, a posebno napredne napadačke vježbe (purple i red testiranja)

· Nadograditi postojeće nadzorne mehanizme rješenjima poput sigurnosnog operativnog centra

ENERGETSKI

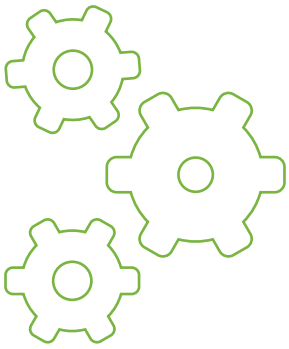
Energetski sektor u današnje vrijeme uvelike ovisi o industrijskim kontrolnim sustavima i sve više uviđa važnost informacijske sigurnosti. Stupanjem na snagu Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, između ostalog, naglašavaju se:

· Procjena rizika kibernetičke sigurnosti

· Obaveze detekcije i prijave incidenta sa značajnim utjecajem

Nadograditi postojeće nadzorne mehanizme rješenjima poput sigurnosnog operativnog centra integralnim pristupom nadzora poslovne i procesne mreže.

PROIZVODNJA



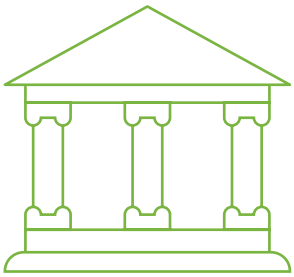
Proizvodni sektor sve više koristi automatizaciju proizvodnih procesa. Uvođenjem automatizacije i međusobne povezanosti sustava putem računalnih mreža u organizacije se uvode novi, dosad neprepoznati rizici. Ti rizici nisu samo rizici IT-a, nego rizici organizacije.

· Prepoznati i tretirati rizike informacijske sigurnosti

· Alocirati dovoljne resurse (ljudske i tehničke) za informacijsku sigurnost

· Izdvojiti informacijsku sigurnost izvan IT odjela

· Podizati svijest zaposlenika o informacijskoj sigurnosti



JAVNI SEKTOR

Pandemija virusa COVID-19 izazvala je krizu u javnom sektoru čije posljedice uključuju prelazak na povećani opseg rada od kuće za većinu javnih institucija. Takvim prelaskom potrebno je osigurati zadržavanje zadovoljavajuće razine usluga i servisa građanima na siguran način. Koko bi to postigli potrebno je:

· Osigurati sigurno spajanje na mrežu institucije korištenjem provjerenih računala i sigurnih protokola spajanja

· Obučiti zaposlenike o rizicima rada od kuće i načinima kako te rizike minimizirati

· Provjeravati ranjivosti i penetracijski testirati izradu novih rješenja koja digitaliziraju usluge

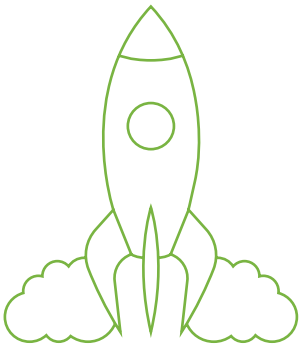
MALOPRODAJA

Pandemija virusa COVID-19 izazvala je krizu i zatvaranje ili ograničenje rada prodajnih lanaca. Ulazimo u vrijeme internetske trgovine, a kako bi internetska trgovina bila sigurna potrebno je da:

· Vođenje projekta izrade ili nadogradnje internetske trgovine uključuje komponentu informacijske sigurnosti kroz životni ciklus

· Treća strana koja pruža usluge izrade programskih rješenja primjenjuje dobre prakse informacijske sigurnosti i zaštite podataka o transakcijama

· Se provodi kontrola nad trećim stranama



START UP

Informacijsku sigurnost najlakše je implementirati prilikom pokretanja poduzetničkog poduhvata. Svakako razmotrite:

· Prirodu poslovanja i ovisnost poslovanja o informacijskim tehnologijama

· Ukoliko poslovanje ovisi o informacijskim tehnologijama, primijenite razumne tehničke i organizacijske mjere koje će umanjiti rizike i koje će vašim korisnicima dati sigurnost i povjerenje prilikom korištenja proizvoda ili usluga

· Educirajte osoblje o osnovama informacijske sigurnosti

· Provodite testiranja IoT rješenja ukoliko ih razvijate

Diverto pruža visoko specijalizirani spektar usluga iz područja informacijske sigurnosti.

Usluge prilagođavamo kako bismo zadovoljili specifične potrebe naših klijenata, s ciljem unapređenja njihove sigurnosti uz najbolji omjer cijene i kvalitete.

W: www.diverto.hr | **E:** diverto@diverto.hr