CERT.hr

grow-cert

Jačanje kapaciteta Nacionalnog CERT-a i poboljšanje suradnje na nacionalnoj i europskoj razini

Projekt: CEF-TC-2016-3 – Cyber Security – Action No: 2016-HR-IA-0085

CARNET

CERT.hr

Sufinancira Europska unija
Instrument za povezivanje Europe

#SurfajSigurnije

Radionica za podizanje svijesti o kibernetičkoj sigurnosti

Autor: CERT.hr

Što štitimo?

- Primarni cilj kibernetičke sigurnosti je sigurnost i zaštita informacija, uređaja i opreme tvrtke te podataka

KAKO? - Postavljanje sustava, procesa i pravila

- Svijest o tome kako je čovjek dio toga i ima pristup tim sustavima
- Kako upravljati lozinkama, osjetljivim informacijama i drugim pitanjima jako je važno za strogi nadzor kibernetičke sigurnosti unutar organizacije

Zašto se štitimo?

- **Krađa podataka** - zlonamjerni program može zaraziti računala i koristiti ih za neovlašteni pristup podacima
- **Korištenje slabosti sustava** omogućava ilegalni i neovlašteni pristup našim sustavima
- **Oštećenje podataka** – neki zlonamjerni sadržaj može šifrirati naše podatke i onemogućiti nam pristup našim datotekama
- **Povjerljivost** naših spremljenih podataka može biti narušena – korisnički podaci mogu biti ukradeni kako bi se stekao neovlašteni pristup informacijama
- **Zlouporaba ili ometanje infrastrukture** – nestanak električne struje u cijeloj zgradi

Razlika između prijetnje i ranjivosti

- Ranjivost je interna slabost sustava na koju možemo utjecati
  - Nemarni ili nesavjesni zaposlenici
  - Zastarjela sigurnosna politika, procesi, procedure ili arhitektura / infrastruktura
  - Neovlašten pristup informacijama

- Prijetnje dolaze izvan organizacije
  - Malware – zlonamjerni programi
  - Phishing napadi
  - Kibernetički napadi s ciljem krađe informacija, podataka ili intelektualnog vlasništva
  - Unutarnji napadi

Kako izgleda napad?

4 osnovna koraka

- Korak 1 – napadač istražuje – ljudi i organizacija
- Korak 2 – izbor metode ili tehnike napada za iskorištavanje ranjivosti
- Korak 3 – izvršavanje napada – napadač kontrolira
- Korak 4 – čišćenje – brisanje dokaza napada iz sustava

Elementi odgovarajućeg programa za upravljanje rizicima kibernetičke sigurnosti

3 osnovna elementa ili razine programa:

- Otežavanje neovlaštenog pristupa – prevencija
- Identifikacija upada / incidenta / napada – smanjenje štete i osiguravanje daljnjeg rada
- Odgovor na incidente i oporavak - obnova i upravljanje poslovnom održivosti

Prevencija i upravljanje rizikom kibernetičke sigurnosti

- Uvid u rizike za organizaciju – što treba zaštititi?
  - Ljudi
  - Oprema – serveri, računala - *Hardware*
  - Programi – *Software*
  - Fizička sigurnost – objekt, zgrada, uredi
- Odluke o ulaganju u zaštitu ciljanih rizika
  - Procjena nastanka i utjecaja pojedinog rizika na poslovanje
  - Uvođenje organizacije u digitalno sigurno okruženje
- Svi zaposlenici trebaju biti svjesni rizika i znati se ponašati u takvim slučajevima

Upravljanje rizicima

1. Procjena rizika započinje s jasnom slikom o imovini i resursima
2. Procjena imovine i resursa – što zaštititi, gdje i zašto?
3. Kreiranje liste rizika
4. Kategorizacija rizika – dobro/imovina – rizik – ranjivost – mogućnost iskorištavanja – vrijednost štete /visoka/srednja/niska
5. Kreiranje liste za ublažavanje rizika i plan upravljanja rizicima
6. Utvrđivanje procesa i tima (organizacija)
7. Analiza utjecaja rizika i proračun

6 osnovnih motiva za podizanje sigurnosti

1. **Interna revizija** – kada se pronađe nešto što nije usklađeno s politikom i poslovanjem tvrtke – cilj podizanje svijesti, interna pravila koja su važna za tvrtku
2. **Vanjska revizija** – kada se pronađe nešto što nije usklađeno s mogućnošću iskorištavanja pronađene slabosti, zakonska pravila
3. **Loš osjećaj** – tvrtka osjeća da se nešto dogodilo, ali ne zna o čemu se radi, treba izgraditi više proaktivni pristup za podizanje svijesti, ulagati u sustav za detekciju problema i prikupljanje dokaza
4. **Incident** – hakiranje – javno obznanjen napad s utvrđenom štetom na resursima ili neobjavljen napad, potrebno je utvrditi kako je došlo do napada, implementacija tehnologije i procesa kako se takav napad ne bi ponovio
5. **Korištenje novih programa** – s njim dolaze i novi rizici, a i pitanje povjerenja u njegovu funkcionalnost i dobavljača
6. **Novi procesi** – koliko su sigurni

Kampanje podizanja svijesti zaposlenika

CILJEVI

- Osposobiti zaposlenike za identificiranje i zaustavljanje neuobičajenih aktivnosti
- Pojasniti sigurnosnu politiku, tim i organizaciju i zašto je to važno (složene lozinke)
- Uključiti ljude kao vitalni dio obrane (i zadržati takav oblik)
- Osigurati opću sigurnost kroz raspravu i prijenos dobrih praksi i informiranje ljudi o rizicima
- Pružanje informacija o dopuštenom i nedopuštenom korištenju resursa kao što su internet, elektronička pošta, baze podataka i prijenos podataka i sl.
- Dovesti ljude do shvaćanja kako se radi i o njihovoj osobnoj sigurnosti

4 zlatna pravila i praktični savjeti

Kako obavljati svoje zadatke ispravno i kako doprinijeti sigurnosti i zaštiti organizacije?

1. Zaštita vlastitog identiteta
    - Korisnička imena i lozinke štite od neovlaštenih pristupa sustavima i osiguravaju pristup samo ovlaštenim osobama
    - Upravljanje lozinkama
        - Provjera lozinke na https://haveibeenpwned.com/
2. Oprezno korištenje e-poruka i interneta
    - Posjećivanje sigurnih web sjedišta
        - Provjera sigurnosti web sjedišta na https://www.circl.lu/urlabuse/
    - Povjerljivost e-poruka
    - Objavljivanje sadržaja na društvenim stranicama

3. Zaštita uređaja

- Vaš uređaj nikad ne smije ostati bez vašeg prisustva
- Vaš mobilni uređaj mora biti zaštićen PIN-om. Ovo je posebno važno ako koristite vlastiti uređaj u poslovne svrhe
- Spajajte svoje uređaje samo na provjerene uređaje za pohranu podataka ili za prijenos podataka
- Ista pravila koristite za privatne uređaje kao i za uređaje koje koristite u poslovne svrhe
- Redovito radite sigurnosne kopije poslovno vezanih informacija koristeći mrežne uređaje
- Ne nosite uređaje koji sadrže informacije o tvrtki sa sobom ukoliko ih ne trebate
- Ukoliko koristite Wi-Fi bežično spajanje spajajte se samo na poznate uređaje i provjerene mreže

4. Budite svjesni svoga okruženja

- Provjerite je li osoba koja zahtijeva pristup ograničenim informacijama ovlaštena za dobivanje tih informacija
- Tiskajte i kopirajte dokumente ili podatke samo kada je to zbilja potrebno
- Koristite poveznice kada dijelite dokumente s nekim kolegama
- Budite svjesni ljudi koji gledaju preko ramena ili prisluškuju
- Spremajte digitalne informacije na USB stickove samo kada je to potrebno
- Ne upravljate i ne koristite se povjerljivim informacijama na javnim računalima
- Budite svjesni ljudi koji ulaze u zaštićene administrativne prostore bez određenog povoda ili razloga

grow-cert

CERT.hr

#SurfajSigurnije

www.cert.hr
www.naivci.hr

https://www.facebook.com/CERT.hr/

https://twitter.com/HRCERT