Prioritetne preporuke za zaštitu od kibernetičkih napada

Smanjivanje površine napada

- Identifikacija servisa koji su javno izloženi/dostupni putem Interneta (npr. web stranice, e-pošta, VPN ulazne točke, nadzorne konzole, RDP ili SSH servisi za udaljenu administraciju, SFTP, SMB i sličnih servisa za razmjenu datoteka, i dr.)
  - pregled javno dostupnih servisa može se dobiti na tražilicama poput *Shodan*, *Censys* i sl.
- Ograničavanje dostupnosti servisa
  - *Primjer1* RDP vjerojatno ne treba biti dostupan preko Interneta već samo nakon VPN-a i ili nekog drugog oblika pred-autentifikacije
  - *Primjer2* ako VPN treba biti dostupan možda postoji mogućnost ograničavanja na pojedine IP adrese ili samo na hrvatske IP adrese i ASN prefikse
- Smanjivanje broja administratorskih i visoko privilegiranih korisničkih računa
  - *Primjer* uklanjanje/onemogućavanje računa koji se ne koriste (računi bivših djelatnika, računi koji nisu izravno povezani s određenom osobom - npr. korisnik "*Administrator*", servisni računi kojima ne trebaju administratorske ovlasti i sl.)
- Blokiranje pristupa servisima s TOR mreže i poznatih anonimizacijskih VPN servisa
- Ograničavanje direktnog pristupa Internetu poslužiteljima
  - *Primjer1* distribuciju nadogradnji provesti interno
  - *Primjer2* DNS rezoluciju proslijediti interno na središnje DNS poslužitelje

Sigurnost lozinki i dvofaktorska autentifikacija

- Zaštita ovlaštenog pristupa putem sučelja za prijavu (Elektronička pošta, VPN, CMS web stranice, ...):
  - dvofaktorskom autentifikacijom (*two-factor authentication*)
  - strogim pravilima za lozinke (*password policy*) - npr. minimalna duljina za lozinke redovnih korisnika je 12 znakova koja moraju biti kombinacija velikih i malih slova, znamenki te specijalnih znakova, za privilegirane korisnike 16 te za servisne korisnike 24
  - mehanizmom za zaključavanje korisničkih računa nakon prekomjernih neuspjelih pokušaja prijave (*account lockout*) uz mogućnost automatskog otključavanja nakon korisniku razumnog perioda radi sprječavanja napada uskraćivanjem usluge
  - osigurati da se korisnička imena i lozinke korištene na servisima s dvofaktorskom autentifikacijom ne koriste na drugim servisima bez dvofaktorske autentifikacije
  - izbjegavanje korištenja istih lozinki na različitim javnim servisima te korištenje službenih adresa na javnim servisima radi smanjivanja rizika od napada
  - izbjegavanje spremanja lozinki u web preglednike
- Posebno je važno zaštititi:
  - javno izložena/dostupna sučelja putem Interneta
  - sučelja koja napadaču omogućuju pristup poslužiteljima ili internoj mreži (npr. VPN)
- Provjeriti vrijeme posljednje promjene lozinke korisničkih računa, posebice lozinki administratorskih računa
  - ako su pravila za lozinke u međuvremenu postrožena, ključno je da se nakon toga ponovno promijene lozinke - inače pravila nisu primijenjena

Primjena sigurnosnih zakrpa

- Odrediti tko je zadužen za primjenu sigurnosnih zakrpa za svaki dio infrastrukture (poslužitelje, mrežnu opremu, sigurnosne uređaje)

- Uspostaviti proces redovne primjene sigurnosnih zakrpa (*security updates/patches*) najmanje jednom mjesečno te dodatno po informaciji o novim kritičnim ranjivostima, a gdje je tehnički moguće omogućiti automatska ažuriranja
- Provjeriti vrijeme zadnje primijenjene sigurnosne zakrpe na svim ključnim dijelovima infrastrukture, ne samo na poslužiteljima, već i na mrežnoj opremi, sigurnosnim uređajima, aplikacijama i slično

Pričuvne kopije podataka (backup)

- Odrediti koji su ključni podaci te osigurati da se redovno rade pričuvne kopije tih podataka
- Najmanje jedna kopija podataka mora biti izolirana od eventualnog napada pohranom u sustav upravljan drugi skupom administratorskih ovlasti ili njenom nepromjenjivosti (*immutable copy*). Ukoliko napadač ostvari administratorske ovlasti (npr. *Domain Admin*), ne smije imati mogućnost šifrirati/izbrisati pričuvne kopije ključnih podataka
- Uspostaviti proces redovne provjere oporavka pričuvnih kopija podataka. Važno je provjeriti obuhvaćaju li pričuvne kopije sve ključne podatke i funkcionira li proces oporavka

Detekcija napada

- Osigurati dostupnost i potpunost dnevničkih zapisa (*logs*) za ključne servise (prijave na VPN, elektroničku poštu, detekcije antivirusnog sustava i drugih sigurnosnih uređaja) za dovoljan vremenski period od barem tri mjeseca
  - *Primjer1* osigurati vidljivost javnih IP adresa u dnevničkim zapisima pristupanja Exchange poslužitelju (npr. omogućiti bilježenje *X-Forwarded-For* polja)
  - *Primjer2* osigurati vidljivost javnih IP adresa, korisničkih imena i dodijeljenih IP adresa u zapisima prijava na VPN
- Osigurati pravovremenu detekciju i obavještavanje (npr. kroz poruku elektroničke pošte ili obavijest) u slučaju sumnjivih aktivnosti na mreži.
  - *Primjer1* detekcija zlonamjernog kôda na poslužitelju
  - *Primjer2* detekcija prekomjernih neuspješnih prijava na VPN ili elektroničku poštu, prijava sa sumnjive IP adrese, IP adrese izvan RH ili u neuobičajenom vremenskom razdoblju

Izdvojene dugoročne preporuke

- Provjera dolazne elektroničke pošte u sustavima za dinamičku analizu (*Sandbox*)
- Segmentacija mreže i ograničavanje pristupa kritičnim servisima
  - *Primjer1* ograničavanje pristupa radnih stanica običnih korisnika servisima za koje nema poslovne potrebe
  - *Primjer2* ograničavanje mrežne dostupnosti računala nakon spajanje putem VPN veze na samo nužne servise
  - *Primjer3* Izuzev potreba spajanja dislociranih dijelova infrastrukture, ograničiti broj site-to-site VPN veza ukoliko je moguće uz primjenu jasne segmentacije, ograničavanja mrežne dostupnosti na samo nužne destinacije i bilježenje pojedinih konekcija
- Uklanjanje manje sigurnih protokola komunikacije i korištenje sigurnih inačica
  - *Primjer1* korištenje POP3 ili IMAP kroz TLS vezu
  - *Primjer2* korištenje SFTP umjesto FTP
- Provjera odlaznog mrežnog prometa korisnika i filtriranje prema nepouzdanim web stranicama