Kako zaštiti imovinu pojedinca i organizacije u cyberspaceu?

Kako bismo zaštitili imovinu svoje organizacije u kibernetičkom prostoru (cyberspace-u) potrebno je prvo razumjeti osnovne pojmove.

Cyberspace ili cyber-prostor definiramo kao složeno okruženje nastalo interakcijom ljudi, softvera i usluga na Internetu, uz pomoć spojene opreme i mreža koje ne postoji u bilo kojem fizičkom obliku.

Cybersecurity tj. kibernetička sigurnost je očuvanje povjerljivosti, integriteta i raspoloživosti informacija u cyber-prostoru.

Na sljedećoj slici prikazan je odnos između cyber-sigurnosti i drugih domena sigurnosti.

Slika 1: Odnos između cyber-sigurnosti i drugih domena sigurnosti

Kada razumijemo osnovne pojmove i odnos između cyber-sigurnosti i drugih domena sigurnosti, trebamo prepoznati prijetnje u cyber-prostoru, mehanizme napada i ključne sudionike.

Prijetnje u cyber-prostoru mogu biti usmjerene na pojedince ili organizacije tj. njihovu imovinu koja može biti u fizičkom ili virtualnom obliku.

Kao mjere za zaštitu imovine mogu se koristiti najbolje prakse u području preventivnog, detektivnog i reaktivnog djelovanja.

Istraživanja su pokazala da je 43% cyber-napada usmjereno na mala poduzeća te da je najskuplja komponenta cyber-napada gubitak informacija koji čini 43% troškova.

Norma ISO 27032 daje uputstva za pripremu cybersecurity programa, čijom implementacijom se može postići željena razina sigurnosti u cyber-prostoru. Norma ukazuje na vrlo kompleksan odnos između cyber-sigurnosti i drugih sigurnosnih domena. Sigurnost cyber-prostora je usko povezana i s Internet sigurnošću, mrežnom sigurnošću i generalno informacijskom sigurnošću. Ova norma polazi od identifikacije imovine u cyber-prostoru i prepoznavanja potencijalnih cyber-prijetnji i rizika te daje smjernice za odabir adekvatnih mjera kojima se umanjuje vjerojatnost ostvarenja cyber-prijetnji.

Prijetnje osobnoj imovini u cyber-prostoru mogu biti krađa ili curenje osobnih podataka, krađa identiteta, prodaja podataka na crnom tržištu, neautorizirani pristup financijskim podacima osobe (krađa novca, prevara), napad na avatar ili virtualnu valutu u svrhu konverzije u stvarne vrijednost, „Virtual theft" i „Virtual mugging", pretvaranje osobnog računala u zombi / bot itd.

Prijetnje organizacijskoj imovini u cyberspace-u mogu biti ugrožavanje integriteta i dostupnosti web stranica organizacije, krađa i preprodaja URL-a organizacije, krađa osobnih podataka zaposlenika, klijenata, partnera i dr., otkrivanje povjerljivih podataka koje rezultira kršenjem regulative i financijskim posljedicama, krađa podataka od nacionalne važnosti kroz e-government servise itd.
Navedene prijetnje žele iskoristiti ranjivosti sustava različitim mehanizmima napada kako bi uništili, otkrili, otuđili, onemogućili, ostvarili neovlašten pristup ili neovlašteno koristili imovinu.

Mehanizmi napada mogu doći unutar privatne mreže ili izvan nje.
Primjer napada unutar privatne mreže je zloporaba administratorskih prava ili korištenje softverskih tehnika i alata (malware, key loggeri itd.), kako bi se došlo do lozinki ili drugih podataka o identitetu unutar privatne mreže.

Napadi izvan privatne mreže ciljaju ono što je dostupno prema van, a to mogu biti routeri, serveri, firewallovi, Web itd. Neki od primjera su „port scanneri" koji skeniraju sve portove na serveru i traže one koji su otvoreni (jedna od svrha im Denial of Service napad pomoću botova). Moguć je i tzv. „buffer overflow" metoda kompromitiranja servera slanjem znatno dužeg niza znakova od očekivanog koja uzrokuje nekontrolirani način rada te omogućava ubacivanje malicioznog koda. Koristi se i „IP spoofing" tj. manipuliranje IP adresama u pokušaju maskiranja u poznati izvor u svrhu ostvarenja neautoriziranog pristupa sustavu.
Također, sve učestalijim korištenjem *peer-to-peer* aplikacija za dijeljenje datoteka (fotografija, glazbe, videa...) napadi postaju sve sofisticiraniji te pokušavaju maskiranjem prenijeti maliciozni kod na druga računala putem „trojanskih konja".

Kako bismo prepoznali koje mjere cyber-sigurnosti implementirati, prvo je potrebno provesti procjenu rizika. Da bismo proveli procjenu rizika potrebno je identificirati kritičnu imovinu jer nije isplativo štititi svu imovinu. Kod procjene rizika organizacija treba odlučiti koju metodologiju će koristiti, a prilikom odabira metodologije može se služiti ISO 27005 normom. Bitno je razumjeti da koju god metodologiju upravljanja rizicima organizacija odabrala, nikad neće spriječiti pojavu svih rizika već će samo prepoznati rizike, njihovu razinu te odabrati način postupanja s rizicima. Opcije postupanja s rizicima su sljedeće:

1. Primjenjivanje odgovarajućih mjera za smanjenje rizika
2. Svjesno i objektivno prihvaćanje rizika (ako on zadovoljava politiku organizacije i kriterije za prihvaćanje rizika)
3. Izbjegavanje rizika
4. Prijenos rizika na druge strane, npr. osiguravatelje ili dobavljače.

Procjenu i upravljanje rizicima potrebno je redovito obavljati, poglavito za područje kao što je cyber-sigurnost, zbog njegove dinamičnosti i učestalih promjena.

Ako se pri postupanju s rizicima organizacija odluči za opciju smanjenja rizika, tada prema normi ISO 27032 može implementirati neke od sljedećih mjera:

- Kontrole na razini aplikacija
    - Kratki prikaz osnovnih online politika
    - Sigurno rukovanje sesijama Web aplikacija (cookies)
    - Sigurnosna provjera inputa (prevencija SQL-Injectiona)
    - Siguran Web scripting (prevencija Cross-site Scriptinga)
    - Pregled i testiranje sigurnosti koda

    - Mogućnost autentikacije usluge od strane korisnika (pod-domena, https...)

- Kontrole za zaštitu servera
    - Sigurnosna konfiguracija servera (kontrola pristupa, logovi...)
    - Implementirati sustav testiranja i podizanja sigurnosnih nadogradnji
    - Nadzor sigurnosnih performansi servera kroz redovit pregled logova
    - Implementacija kontrola protiv zlućudnog koda na serveru (anti-virus, anti-spyware)
    - Provedba testiranja ranjivosti online aplikacija

- Kontrole za krajnje korisnike
    - Korištenje podržavanog operativnog sustava i aplikacija, s redovito ažuriranim sigurnosnim zakrpama
    - Korištenje anti-virus i anti-spyware alata
    - Omogućavanje blokiranja skripti / prihvaćanje skripti samo iz provjerenih izvora
    - Korištenje phishing filtera
    - Korištenje osobnog vatrozida i HIDS
    - Korištenje drugih raspoloživih sigurnosnih karakteristika Web preglednika, omogućavanje automatskog ažuriranja itd.

- Kontrole za zaštitu od napada socijalnog inženjeringa (učinkovita zaštita kao kombinacija)
    - Sigurnosnih politika
    - Metoda i procesa za:
        - Klasifikaciju informacija
        - Osvješćivanje i edukaciju
        - Testiranje
    - Organizacije i ljudi
    - Tehničkih kontrola

- Kontrole za unapređenje spremnosti cyber sigurnosti
    - Darknet monitoring (skup IP adresa koje se ne koriste u organizaciji)
    - Black Hole Monitoring
    - Low i High Interaction Monitoring
    - Sinkhole Operation (preusmjeravanje specifičnog IP prometa prema „sinkhole" uređaju)
    - Traceback (rekonstrukcija puta napada, lociranje napadača, korekcija prometa...)

Organizacija može svoju razinu cyber-sigurnosti dodatno unaprijediti koristeći i preporuke iz drugih raspoloživih metodologija i okvira, kao što su ENISA, NIST Cybersecurity Framework itd.
Kako bi cyber-security program organizacije davao željene rezultate i stalno se unapređivao,potrebno je redovito provoditi procjenu rizika te pratiti promjene u okruženju i pojavu novih prijetnji kao i promjene ranjivosti do kojih može doći zbog promjena u poslovanju, ciljevima ili imovini.