MIKÄ ON KYBERPUOLUSTUKSESSA RIITTÄVÄ TASO?

Riittävän ratkaisun rakentaminen

nixu

AGENDA

- Puolustajien eri menetelmät
- Hyökkääjät, motivaatio ja tavat
- Kun tietomurto tapahtuu
- Reaaliteettien tarkastus
- Riittävän puolustuksen rakentaminen
  - Pilvipalveluiden suojaaminen

nixu

PUOLUSTUSMENETELMÄT

- Palomuurit verkon reunoille
  - Myös sisäreunoille, jos niitä on
- Minimoi hyökkäysalue
  - Kovenna käyttöjärjestelmä
  - Kovenna ohjelmisto
- Päivitä ohjelmistoa jatkuvasti
- Aja antivirusohjelmistoa Windows järjestelmissä
- Varmuuskopiointi
- Salasanojen kompleksisuus vaatimukset & vaihtaminen usein
- Käyttäjien kouluttaminen
- Tiedon salaus
- Verkkoliikenteen valvonta
  - IDS / IPS
- Haavoittuvuusskannaukset
- Hyökkäystestit (pentesting)
- SIEM
  - Threat intelligence
  - Verkkoliikenteen analysointi

nixu

YLEISIMMÄT HYÖKKÄÄJÄT JA MOTIVAATIO

- Taloudellista etua hakevat erilaiset ryhmät
- Omat työntekijät
- Hyökkääjien motivaationa on 89% tapauksista joko taloudellisen edun saaminen tai yritysvakoilu.
  - ~80% on taloudellinen etu
  - 9 % on vakoilu
  - 11% jotain muuta
- Toissijaiset motivaatiot, eli sivuston käyttö haittaohjelmien jakoon, DNS:n väärinkäyttö jnpp tapahtuu niin usein, että ei ole esillä tässä datassa

Ref Verizon 2016 Data breach investigations report

nixu

MITEN?

- Käyttävät valmiita hyökkäyspaketteja, jotka hyödyntävät tunnettuja vanhoja haavoittuvuuksia
  - Massaa vastaan – kohde ei ole merkityksellinen, tulos on
- Vakiotunnuksia tai vuodettuja salasanoja ja käyttäjätunnuksia
  - Kohdennettuna vuodettujen tunnusten avulla
  - Massaa vasten vakiotunnusten kanssa
- Vanhaa kunnon sosiaalista hakkerointia
  - Sähköpostit ja feikkisivustot

nixu

I AM CONVINCED THAT THERE ARE ONLY TWO TYPES OF COMPANIES:
THOSE THAT HAVE BEEN HACKED AND THOSE THAT WILL BE. AND EVEN THEY ARE CONVERGING INTO ONE CATEGORY: COMPANIES THAT HAVE BEEN HACKED AND WILL BE HACKED AGAIN.

- FBI JOHTAJA ROBERT S. MUELLER, III (MARCH 01, 2012)

NIXU

KUN TIETOMURTO TAPAHTUU, SE ON NOPEASTI TEHTY

- Murto tapahtuu hyvin nopeasti, minuuteissa
- Automatisoitu työkalu käyttää tunnettua haavoittuvuutta päästäkseen alustalle, jonka jälkeen se ottaa yhteyttä C&C palvelimille ja odottaa jatkotoimia
- Käyttäjä avaa sähköpostin liitetiedoston, jossa oleva haittaohjelma alkaa seuraamaan käyttäjän toimia
    - Käyttäjätunnusten kopiointi (key loggers, memory scapers)

nixu

KUN TIETOMURTO TAPAHTUU, SE ON HITAASTI HAVAITTU

193 PÄIVÄÄ

Keskimääräinen aika, jossa tietomurto HAVAITAAN

.

69 PÄIVÄÄ

Keskimääräinen aika, jossa tietomurto SAADAAN HALLINTAAN.

~70%

tietomurroista havaitaan ULKOISEN TOIMITSIJAN TOIMESTA.

Sources: Verizon Data Breach Investigation report 2016, 2016 Cost of Data Breach Study: Global Analysis. Ponemon Institute.

nixu

ONKO MAAILMA OIKEASTI NÄIN SYNKKÄ?

- Maailma ei ole niin synkkä paikka kuin tilastot näyttävät tai FBI:n entinen johtaja sanoo.
- Hyökkääjät ovat valtavalta osin opportunisteja helpon rahan perässä
  - Heitä vastaan voidaan suojautua perusasioilla
  - Tämän tyyppinen toiminta voidaan havaita, jos valvonta on olemassa
- Harvinaisissa erityistapauksissa hyökkääjät ovat metsästämässä juuri sinua, jolloin maailma on oikeasti synkkä.

nixu

MIKÄ ONTUU?

- Tilastojen mukaan, pääasiassa
  - Päivitykset roikkuvat perässä, pahasti
  - Käyttäjätunnusten käyttöä ei havaita lainkaan
    - Hyökkääjät haluavat käyttää normaaleja tunnuksia, sekä normaaleja ylläpitotyökaluja sillä ne ei aiheuta hälytystä tai epäilyjä
- Valvonta, pahasti
  - Verkkoliikennettä ei nähdä
  - Käyttäjätunnusten käyttöä ei nähdä

nixu

Riittävän kyberpuolustuksen rakentaminen

nixu

OPPORTUNISTISTEN HYÖKKÄYSTEN PYSÄYTTÄMINEN

- Jatkuva päivittäminen
  - Halvalla ostettavat valmiit hyökkäyspaketit hyödyntävät tunnettuja jo estettävissä olevia haavoittuvuuksia.
  - 0-päivä haavoitettuudet on hinnaltaan liian kovia ja vain harvojen käytössä.
  - Ei pelkästään käyttöjärjestelmä, vaan myös varsinaiset ohjelmistot – mukaan lukien ohjelmistojen lisäosat (vrt Wordpress ja sen lisäosat)
- Käyttäjätunnusten hallinta
  - Vakio salasanat pois (kaikista laitteista)
  - Vahva salasana / toisen tekijän tunnistautuminen käyttöön
  - Ylläpito-oikeudet erillistunnuksille, pois päivittäiseltä käyttötunnukselta
  - Pilvipalveluiden tunnusten eriyttäminen, logit toisen tilin hallintaan – ei sen jota valvotaan.

nixu

OPPORTUNISTISTEN HYÖKKÄYSTEN PYSÄYTTÄMINEN

- Palomuurit
  - Myös pilvipalveluissa
- Tiedon salaus
  - Läppäreissä ja kännyköissä
- Viruksentorjunta
  - Haittaohjelmia syntyy joka sekunti, jokaista ei saada kiinni aina, mutta hieman vajaa suojaus on parempi kuin ei mitään suojausta.
- Käyttäjän koulutus on tärkeää, mutta haittaohjelmatartunta ei ole käyttäjän vika.
  - Jokainen meistä saa sähköpostitse Word, PDF, Excel, dokumentteja melkein päivittäin. Jos yksi sadasta tai tuhannesta on haitallinen, ei voida olettaa käyttäjän arvioivan jokaista samalla pieteetillä

nixu

ONNISTUNEEN HYÖKKÄYKSEN KÄSITTELY

- Valvonta
  - Vähintään
    - tunnistustapahtumien kerääminen ja analysointi
    - Verkkopalvelimien tapahtumien / liikenteen seuranta
  - Mahdollistaa murron vaikutusalueen selvittämisen, mahdollisesti hyökkääjän jäljittämisen.
- Varmuuskopiointi
  - Yrityksen toiminnalle oleellisen tiedon varmuuskopiointi jatkuvalla tasolla
  - Varmuuskopiointia ei ole tehty, ellei tiedon palautusta ole koitettu tehdä sekä ajoittain koiteta tehdä uudelleen.

Pilvipalveluiden suojaaminen

nixu

PALVELUT PILVESSÄ

- Ohjelmistojen päivittäminen pilvessä!
  - erityisesti itselisätyille lisäosille
- Palomuurit (security groups)
- Käyttäjätunnusten hallinta
  - Ylläpitotili on eri tili kuin päivittäinen palvelimien hallintatili
  - Toisen tekijän tunnistautuminen käyttöön

⇒ Onneksi valvonta on kohtalaisen helppoa pilvessä:

- ⇒ Amazon AWS: CloudTrail ja CloudWatch
- ⇒ Microsoft Azure: Security Center

nixu

Riittävän kyberpuolustuksen rakentaminen

Vielä kerran

nixu

PUOLUSTUS LYHYESTI

- Päivitä, päivitä, päivitä
  - (käyttöjärjestelmä) (ohjelmisto) (ohjelmiston lisäosat)
- Käyttäjätunnukset ja salasanat haltuun
  - Vakio salasanat pois
  - Vahva salasana / toisen tekijän tunnistautuminen käyttöön
  - Ylläpito-oikeudet erillistunnuksille, pois päivittäiseltä käyttötunnukselta
- Viruksentorjunta
  - Windows ja OS X koneille
  - Sähköposti- ja levypalvelimelle
- Valvonta
  - Vähintään tunnistustapahtumien valvonta
  - Verkon reunalla olevien palvelimien tapahtumien seuranta

nixu

nixu
cybersecurity.

www.nixu.com

/nixuoy

@nixutigerteam

/company/nixu-oy