Sikkerhedstendenser i 2017 - Et kig i krystalkuglen

Her kan du læse om de vigtigste tendenser på IT Sikkerhedsfronten i 2017 samt om, hvordan du kan bruge Drawares omfattende kendskab til processer og løsninger til at sikre dig mod malware og forberede din virksomhed på at være "compliant" med persondataforordningen, når den træder i kraft i maj 2018.

Vi er i midt i en periode med større udbredelse af digital forretning og administration. Vores afhængighed af digitale systemer bliver mere og mere synlig i takt med at cybersikkerhed bliver udfordret af kriminelle, der forsøger (desværre med stort held) at kompromittere vores (it)sikkerhed for egen økonomisk vindings skyld.

De eksisterende IT-Sikkerheds systemer såsom anti-virus og firewalls er ikke længere tilstrækkelige til at forhindre IT-Sikkerhedsbrud og samtidigt sætter den nye persondataforordning (GDPR) fokus på de lovmæssige regler for at forhindre, kommunikere og håndtere IT-Sikkerhed.

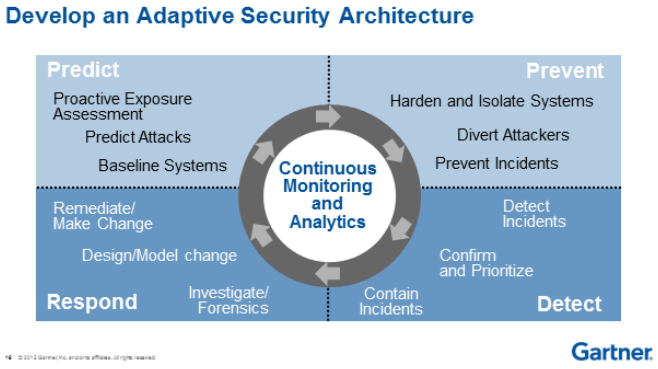
Det betyder, at virksomheder skal ruste sig i væsentligt større omfang end tidligere og tilføre området for IT-Sikkerhed væsentligt større ressourcer - når det gælder:

1. Interne processer til behandling af (person)følsomme oplysninger
2. Nye værktøjer der kan komplementere de traditionelle forsvar mod cyber- og intern kriminalitet
3. Viden om IT-Sikkerhed og mulighed for at bruge den. Internt såvel som eksternt.
4. Et skift fra REAKTIV IT-Sikkerhed til PROAKTIV IT-Sikkerhed

De nuværende modeller for IT-Sikkerhed som fx CIA (Confidentiality, Integrity and Availability) skal suppleres med mindst en gren, nemlig Safety hvor personers og områders sikkerhed kommer til at afhænge af vores håndtering af følsomme oplysninger, vores evne til at forhindre angreb samt vores parathed til at håndtere angreb, når de alligevel forekommer – noget der ligger i hjertet af den nye persondataforordning (CIAS).

Et IT-Sikkerhedsbrud tager i gennemsnit 170 dage at opdage og i mange tilfælde rapporteres det først efter adskillige år! (Se fx listen med anmeldte datasikkerhedsbrud på http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ og https://www.identityforce.com/blog/2016-data-breaches) og datasikkerhedsbristen opdages kun i 69% af eksterne kilder.

Der er derfor brug for at adoptere en metodik (som fx Gartners "Adaptive Security Architecture" (se billedet herunder) som basis for en IT-Sikkerhedsplan "CSIRP", der er grundlaget for et IT-Sikkerheds team "CSIRT" og deres arbejde. Drawares IT-Sikkerhedsbog giver anvisninger på hvordan disse metodikker formes (http://www.draware.dk/om-os/nyhedsarkiv/32-events-temaer/189-event-1).



Prevent > Detect > Respond > Predict (Forhindre > Opdage > Agere > Forudsige)

Tendensen for de kommende år er at fokusere mindre på at blokere og forhindre IT-Sikkerhedsbrister og mere på at kunne opdage, prioritere, undersøge og dokumentere disse brister. Specielt dokumentationen og håndteringen er centrale for persondataforordningen og har baggrund i artikel 32-52. Her er tale om en frist for anmeldelse af en IT-Sikkerhedsbrist, der involverer personfølsomme data, til myndighederne inden for 72 timer. (http://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX%3A32016R0679). Denne proces skal i stigende grad være baseret på en intelligent udlægning af, hvordan hacking aktivitet opfører sig (Behaviour) i stedet for kun at genkende kode/processer, som kendes i forvejen. På den måde bliver du ikke offer for (så mange) zero-day angreb.

I mere specifikke termer vil følgende IT Sikkerhedsområder se en væsentlig vækst i 2017:

A) **Ransomware**

Problem: Et angreb af Ransomware kan være alt fra irriterende over tidskrævende til direkte katastrofalt. Det bliver nemmere og nemmere for IT kriminelle at søsætte Ransomware angreb, fordi disse kan købes på det mørke net som services (Ransomware As A Service "RAAS") og fordi de fleste virksomheder stadig bruger AV som endpoint security og derfor er sårbare overfor Ransomware. Ransomware bliver også mere avanceret og "ondsindet". F.eks. giver nogle af de seneste versioner den ramte mulighed for at sende Ransomware videre til andre brugere og når de bliver ramt, slipper afsenderen for at betale "løsesummen"! Ransomware orme giver anledning til andre typer af infektioner end "bare" kryptering af filer såsom RATs, der installeres så ramte endpoints bliver del af et botnet. Desuden vil den øgede aktivitet fra ikke professionelle IT kriminelle, der drages af RaaS betyde, at brugerne i mindre og mindre grad vil tro på, at en betaling fører til at data afkrypteres.

Løsning: Vi anbefaler, at du bruger en intelligent endpoint security løsning, der ikke blot er afhængig af signaturer (SentinelOne) eller er en klassisk teknologi som Application Whitelisting (HEAT HEMSS). Det er også vigtigt at uddanne brugerne, så de ved, hvad de ikke skal "klikke på" (Wombat Security eller KnowBe4). Sidst men ikke mindst er det vigtigt at kunne dokumentere, at et angreb er i gang og hvad der førte til et Ramsomware angreb (SIEM som fx EventTracker og IBM QRadar)
Dokumentation: Se dokumenterne på vores hjemmeside (http://www.draware.dk/om-os/nyhedsarkiv/123-ransomware) eller på Radware (http://www.radware.com/cyberransomebook/?utm_source=slidernav&utm_medium=slider&utm_campaign=CyberRansomEbook)

B) **Spear Phisning**

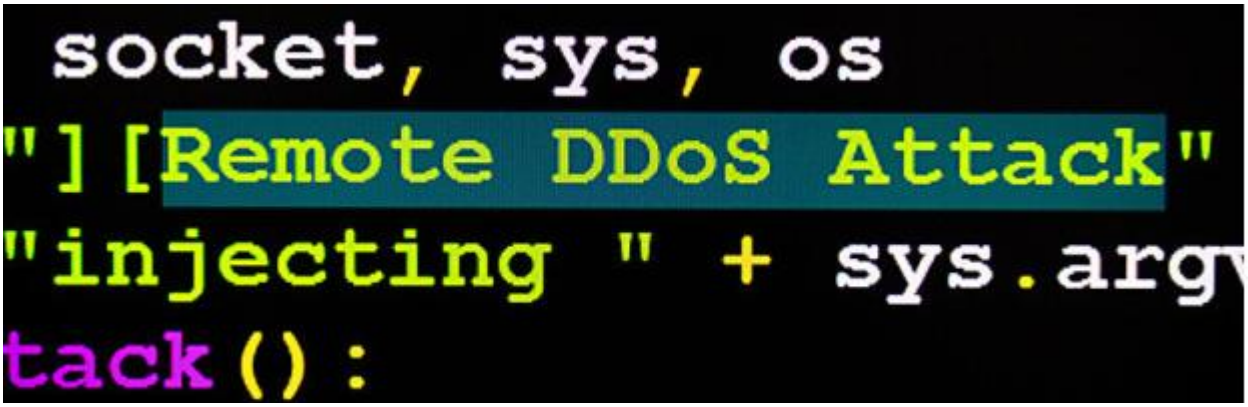
Problem: Trods SPAM firewalls, Antivirus og IPS systemer kommer der stadig e-mails til brugere, der forsøger at lokke brugeren til at klikke på et link, som er porten til et malwareangreb. Det bliver i stigende grad sværere at genkende disse falske mails, eftersom de bliver "bedre" grafisk og på fornuftigt lokalt sprog. Selv for eksperter kan det kræve en sandbox for at afgøre, om der er tale om et malicious link. Denne tendens vil udvikle sig til en endnu større epidemi i 2017. Problemet med falske e-mails bliver større i takt med, at mange større sites mister op til millioner af brugerdata og først offentliggør dette flere år efter sikkerhedsbristen. Se links i starten af denne artikel.

Løsning: Uddannelse af brugerne således at de opnår en større indsigt i, hvad man skal klikke/svare på og hvad man skal holde sig fra (awareness) er centralt. Her er det afgørende at vælge en løsning, som gør det nemt at teste brugernes indsigt i kampagner på lokalt sprog. Dette skal være forbundet med uddannelse så snart brugere klikker på en test phishing mail (Wombat security). Læs gerne producentens "Beyond The Phish" rapport på producentens hjemmeside for mere information om dette emne.

C) **Kendte sårbarheder**

Problem: Antallet af sårbarheder i OS og tredieparts programmer vokser støt år for år, men prioriteringen af sårbarhederne og rettelsen af sårbarhederne kan ikke følge med. Det betyder at specielt tredieparts løsninger fra fx Adobe, Java, Browsere m.fl. forbliver sårbare og derfor udgør væsentlige sikkerhedshuller, der nemt kan udnyttes i phishing og følgende malware kampagner. Fokus på prioritering, rettelse og måling af effektivitet vil føre til en større udbredelse af systemer til vulnerability management. Disse data vil også få en større rolle at spille som grundlag for at sætte relevans på alarmer i SIEM systemer. Desuden vil fokus på patchning af specielt tredieparts programmer vokse.

Løsning: Der er brug for automatiserede løsninger til patch management, som på én gang kan håndtere forskellige OS, standard software fra Microsoft som fx Microsoft Office og tredieparts software (HEAT HEMSS og ManageEngine DesktopCentral). Desuden vil løsninger fra Vulnerability verdenen fortælle og prioritere, hvilke sikkerhedshuller, der skal rettes manuelt og hvilke, der kan rettes automatisk (Tennable Nessus og Rapid7 Nexpose). Viden om sårbarheder, der er blevet udnyttet i live angreb for nylig (se fx Recorded Future) fører til, at virksomheder kan bruge rettelser af sårbarheder mere proaktivt i stedet for den sædvanlige (stærkt forsinkede) reaktive patch management eller pen-tests, hvor resultatet gemmes væk i en skuffe.



D) **DDoS (Distributed Denial of Service) angreb**

Problem: DDoS som en service og den store udbredelse af sårbare IoT gør det nemmere, hurtigere og mere effektivt at udføre DDoS angreb i hidtil uset stor skala. Den meget store båndbredde helt op til 400Gbps til 1Tbps bliver normen ,og de fleste virksomheder - og vel dårligt nok ISPer - kan modstå sådan et angreb. Det kan i længere tid lægge en virksomhed, en offentligt service eller måske vigtige infrastruktursystemer ned. Tendensen for 2017 ser ud til at være et skift væk fra "Stateless" angreb via UDP til Stateful TCP attacks og angreb på applikationslaget fx via http POST. Den kendte mekanisme med mere DNS eller NTP forøgelse af angrebets styrke lever i "bedste" velgående.

Løsning: Det er vigtigt, at du kan opdage, at du er blevet ramt af et DDoS angreb og har forberedt virksomheden på, at dette kan ske. Vi anbefaler, at du bruger SolarWinds Orion til at overvåge svartiden på dine gateway enheder og laver en alarm, hvis de viser en usædvanlig stigning i svartid. Du bør nok også overveje at have en aftale med din ISP om, hvordan du skal reagere som svar på et DDoS angreb og høre, om de mekanismer til DDOS-Scrubbing, du har i virksomheden og i skyen, er tilstrækkelige. Du kan læse mere i dette udførlige dokument (led efter dokumentet "DDoS Attack" på radware.com på Google).

E) **Internet of Things (IoT)**

Problem: Fra enheder, der bruges til personlige formål så som temperaturmålere og fitnessmålere, over enheder, der fungerer i det offentlige rum som fx parkometre, til enheder, der bruges til medicinske formål eller transport som fx biler og fly, har de alle det til fælles, at de ofte er sårbare overfor cyberangreb, fordi de sjældent eller slet ikke opdateres og yder meget lidt modstand overfor et angreb. De kan bruges som zombie devices til Botnets og DDoS angreb eller kompromittering af virksomhedens sikkerhed, fordi de "flyver under radaren". Altså i stedet for Internet of Things (IoT) kan denne kategori af enheder nemt blive Internet of Malicious Things (IoMT)…

Løsning: Her er der desværre dårligt nyt. Der findes typisk ikke specifikke løsninger, så alt hvad man kan gøre er at have fokus på problemet.

F) **Malware as a Service**

Problem: I takt med at malware bliver tilgængeligt for ”hobby hackere” og let kan købes til at foretage selv specifikke angreb, vil 2017 formodentligt byde på langt flere angreb, der udføres af ikke professionelle aktivister, der blot søger en nem økonomisk gevinst. Her kan der fx være tale om DDOS angreb eller Ransomware angreb.

Løsning: De sædvanlige løsninger som nævnt i punkt 1 samt en væsentlig større fokus på malware vil være virksomt.

G) **Synlighed af (person)følsomme oplysninger**

Problem: Med indførelsen af den nye persondataforordning bliver der igen sat fokus på at følsomme oplysninger ikke må være tilgængelige for uvedkommende. Dette gælder ikke kun i elektronisk form men også papirer på et skrivebord efterladt efter arbejdstid eller i frokostpausen samt oplysninger skrevet ned på et whiteboard, som er synlige for en drone gennem et vindue.

Løsning: Nye procedurer skal indføres (dokumenteres og efterprøves) som tager højde for bl.a. disse tilfælde

H) **(Fra)valg af softwareløsninger baseret på Open Source**

Problem: Softwareløsninger baseret på open source er populære, fordi de ofte er billigere, men de er også ofte forbundet med sårbarheder i en platform, der ikke nyder samme frekvens af rettelser. Det har hackerne allerede fundet ud af og derfor betaler det sig bedre at lave angreb baseret på sårbarheder i open source programmer. Disse programmer er desuden ofte grundlaget for operationelle systemer til fx IoT enheder, der så bliver IoMT enheder.

Løsning: Vælg en software platform, som bliver opdateret hyppigt, så sårbarheder kan rettes hurtigt og effektivt – og gerne er automatisk (HEAT HEMSS)

I) **Et større fokus på IT-Sikkerhed**

Problem: Persondataforordningen, som forventes at erstatte den danske data lov fra januar 2018 og få opsættende virkning fra maj 2018, vil forandre det fokus, mange danske virksomheder og myndigheder har på IT Sikkerhed. Det betyder, at der vil blive afsat mere tid, mere HR og større budgetter til at få indarbejdet de processer (fx CSIRP), den organisation (fx CSIRT) og de værktøjer (fx SIEM), der skal til for at understøtte de nye lovkrav. Det vil samtidigt afsløre, at der er et gab mellem den viden om IT-Sikkerhed, der er brug for i virksomhederne, og den viden, som findes blandt virksomhedens tilgængelige ressourcer. Et større fokus på uddannelse indenfor It-Sikkerhed og en større brug af eksterne ressourcer (fx SOC) vil være det mest sandsynlige resultat.

Løsning: Til at understøtte persondatalovens artikel 32-35 om oplysningspligt ved et sikkerhedsbrud, der involverer personfølsomme oplysninger og generel dokumentation, skal man bruge en løsning, som holder styr på alle de hændelser, der er sket på IT infrastrukturen – med andre ord hvem, der har tilgået hvilke data, hvornår og hvordan. Her skal man bruge et log management eller SIEM værktøj (EventTracker eller Correlog eller AD Audit). Der skal desuden afses ressourcer til implementering og drift af et sådant system!