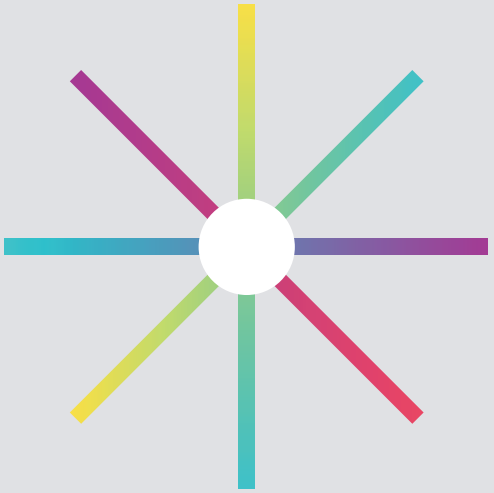
Vejledning i internetsikkerhed for 2018:

Hackerne og forsvaret styrer design og maskinlæring

Indholdsfortegnelse
Indhold



I hele verden er folks liv og levebrød i stadig højere grad rykket online, de fysiske og digitale verdener er ved at overlappe hinanden, og digitale valtuer uden nogen fysisk ækvivalent kan bruges til at købe fysiske varer og serviceydelser. Kunstig intelligens driver beslutningstagningen om selvkørende køretøjer, finder hver eneste dag nye lægemiddelkandidater og tilpasser lektioner, der hjælper elever med at lære.[1,2,3] Samtidig udfører læger livsvigtige operationer på den anden side af verden via internettet og robotter, mens sensorer i netværk ændrer betingelserne for brancher lige fra elproduktion til offentlig transport.[4] Hvert eneste år bliver listen over brancher, der disruptes af sensorer, intelligente maskiner og mikroprocessorer, længere og længere.

Det eneste,der ikke ændrer sig, er, at kriminelle og politiske aktører med onde hensigter forsøger at udnytte svagheder for egen vindings skyld. Og mange af de værktøjer og teknikker, der giver samfundet så store fordele, gør det også lettere at udrette skader, der bliver mere omfattende. Malware, phishing og DDoS-angreb (distributed denial of service) er blot nogle få af de tricks, som er resultatet af de teknologiske landvindinger, der gør verden mere avanceret.

For eksperter i it-sikkerhed kan organisering af vellykket forsvar mod de mange onlineangreb, der nu sker nonstop, være et mareridt, men det kan også være motiverende. Hvem vinder – angriberne eller forsvaret?
Det er svært at bedømme ud fra den daglige sværm af vellykkede angreb, der gør virksomheders drift besværlig og koster millioner af dollars i faldende aktiekurser.[5]

For at sætte fokus på den nuværende og fremtidige situation inden for internetsikkerhed, har vi talt med eksperter på området for at udarbejde denne opdaterede vejledning. HP har lyttet til nogle af de største eksperter i informationssikkerhed for at hjælpe beslutningstagere med ansvar for informationssikkerhed i mellemstore og store virksomheder med at forstå alle de muligheder, de har for at forhindre skader på grund af manglende it-sikkerhed.

Afsnit 1:

Sådan ser situationen ud

Der vil dukke en ny type malware op på internettet hvert fjerde sekund.

I dag vil der blive registreret mellem 6 til 11 millioner nye malwareinfektioner på computere, der kører blot en enkelt type antivirussoftware.[6] Der vil blive igangsat omkring 700 phishingangreb i håb om at lokke folk til at klikke på et bedragerisk link, så en svindler kan stjæle vedkommendes persondata eller få adgang til en virksomheds netværk.[7] Der vil dukke en ny type malware op på internettet hvert fjerde sekund.[8]

Et ukendt antal hackere vil bruge cirka 150 $ på at leje et botnet i en uge for at starte et DDoS-angreb (denial of service), der har til formål at nedlægge en onlinetjeneste eller et onlinenetværk ved at oversvømme det med trafik[9]. På verdensplan bruger disse angreb regelmæssigt 500 gigabit data pr. sekund som våben mod virksomheders og offentlige myndigheders servere for at sluge netværksbåndbredden og tvinge målene for angrebet i knæ.[10,11]

I mellemtiden vil millioner af pc'er og netværkstilsluttede printere, kameraer, termostater og andre IoT-enheder være ubeskyttede, fordi de seneste sikkerhedsrettelser ikke er installeret. Derfor er det kun et spørgsmål om tid, før en ondsindet person får adgang til organisationens mest følsomme data.[12]

Dette har medført en konstant strøm af nyheder om vellykkede angreb på netværk, der egentligt burde være sikre. Blot inden for de første par dage i 2018 lukkede ransomware et regionalt hospitalsnetværk ned for at få en betaling i bitcoin, mens en lokal myndighed og alle computersystemer i en amerikansk skole blev ramt.[13,14,15] På samme tid blev der fundet en meget stor sårbarhed i mikrochip, der kan betyde, at hver eneste moderne computer, der ikke har fået en sikkerhedsrettelse, er sårbar.[16]

Det er tydeligt, at disse angreb – hvoraf alle stort set er økonomisk motiverede – ikke kun er målrettet mod grupper, f.eks. datatyveriet t i Indien i 2016, eller større organisationer som f.eks. Sony, Equifax og Yahoo.[17] Hackerne vil også gerne afpresse små og mellemstore virksomheder, udbydere af sundhedspleje, kommunale myndigheder og andre netværk.[18]
Faktisk er det økonomiske incitament så stort, at truslen kun bliver værre. Ifølge en analyse vil udgifterne i forbindelse med it-kriminalitet i 2021 være 6 billioner $. Ja, du læste rigtigt: billioner. Det er mere end fortjenesten ved salg af narkotika i hele verden.[19]

Se ikke bort fra det indlysende

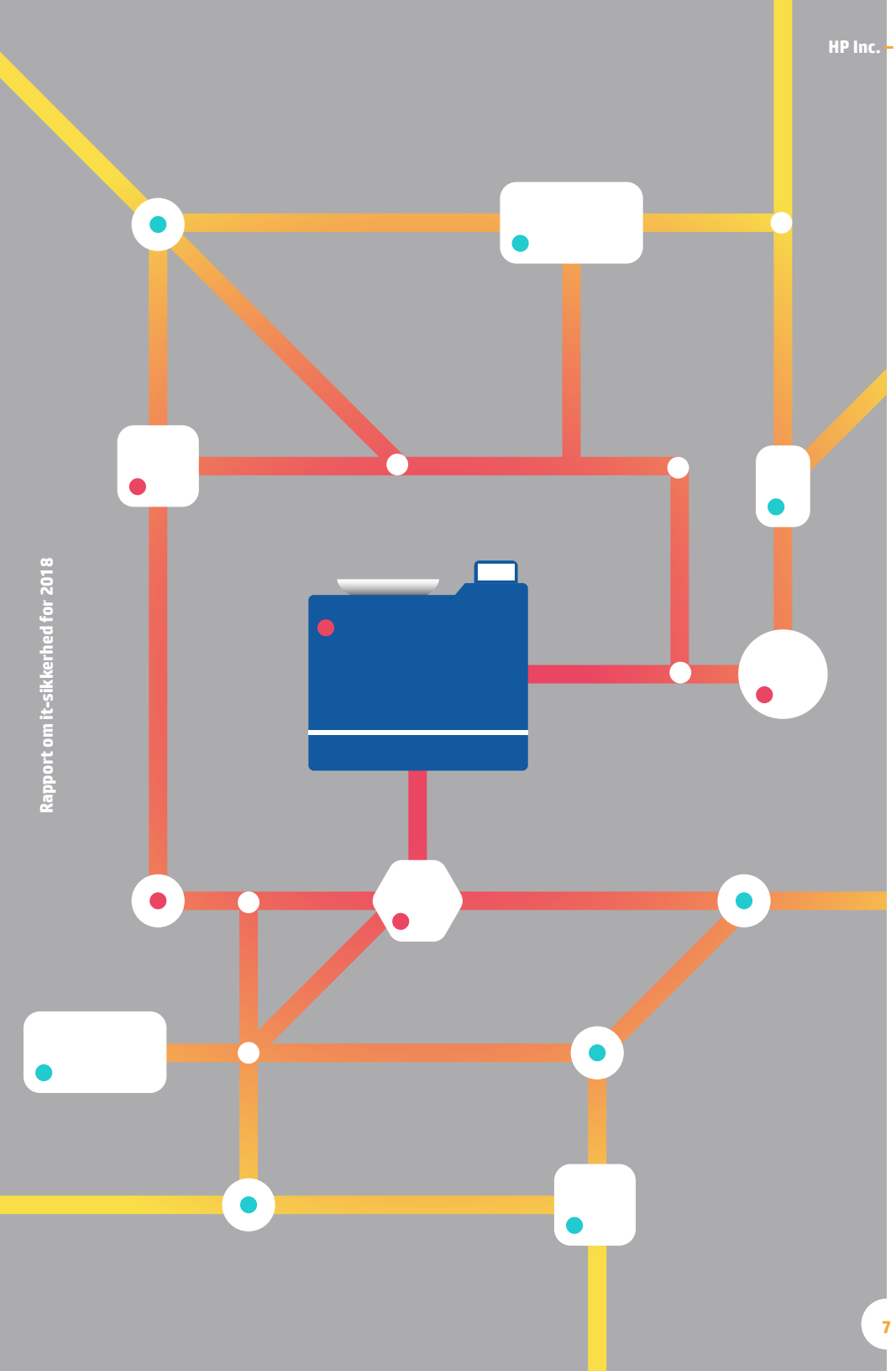
Jason O'Keeffe, som er en af HP's eksperter i printersikkerhed, er ekspert i informationssikkerhed og kender disse trusler alt for godt. Han ved, at forbryderne får masser af hjælp, fordi computere bruges skødesløst, og fordi de installerede it-sikkerhedsforanstaltninger ikke er gode nok, hvilket skyldes, at organisationer enten ikke har it-sikkerhedspersonale, eller også har deres personale ikke ressourcer.[20]

I forbindelse med vurderingen af sårbarheder på virksomheders computernetværk har O'Keeffe set alle typer problemer, der gør livet nemmere for en hacker, samtidig med at han har konstateret åbenlyse mangler i it-afdelingerne, der burde vide bedre.

Under en sådan vurdering blev O'Keeffe bedt om at kigge lidt nærmere på it-infrastrukturen hos en kæmpestor producent. Blandt mange problemer kunne han se, at den fabriksindstillede standardkode ikke var blevet ændret på 90 procent af virksomhedens 36.000 printere i netværket, så alle med den rigtige viden kunne omgå al sikkerhed på enhederne. Da O'Keeffe undersøgte sagen nærmere, kunne han se, at mange printere var konfigureret forkert, så eksterne personer kunne få adgang til printere og konfigurere dem til at stjæle data fra netværket eller hijacke dem og bruge dem i et botnet. O'Keefe kan huske, at deres vicedirektør slog i bordet og sagde: "Jason, tager du gas på mig?". Han havde fråde om munden.

Den hurtige udbredelse af IoT-enheder og andre maskiner, der er tilsluttet både internettet udadtil og virksomhedens interne netværk uden krav om den rigtige godkendelse, betyder, at ondsindede personer hurtigt kan få mange adgangspunkter. Den tid, hvor en it-sikkerhedschef kunne mene, at arbejdet var overstået, når først de kritiske servere i hjertet af virksomhedens aktiviteter var tilstrækkeligt beskyttet, er forbi. Nu skal sikkerhedsapparatet omfatte millionvis af tilsluttede enheder på fjernkontorer – og i medarbejdernes lommer.

"Vi forsøger at beskytte pc'er, servere og andre vigtige dele af netværk, men nu er det IoT-enhederne, der udgør den største risiko for netværk", siger Shivaun Albright, HP's Chief Technologist for Print Security.[21] "Der er typisk en fejl, hver gang der er 100 linjer kildekode. Det eneste, en hacker skal gøre, er at finde en fejl, der giver adgang til systemet. Vi vil gerne sikre os, at vi reducerer antallet af disse udsatte punkter mest muligt."



Adgang hvor som helst

Det er udsigten til en enorm fortjeneste, der får hackere til at tænke i nye baner og være kreative. Ifølge Albright er botnets en af de største trusler, dvs. de automatiserede værktøjer, der bygges ved hjælp af tusindvis af hackede IoT-enheder. For at skabe et botnet hijacker bedragerne processorne på ubeskyttede maskiner og bruger derefter de kompromitterede enheder til at udvinde bitcoin. De kan også udleje deres botnet til andre, der gerne vil starte DDoS-angreb mod tilfældige ofre.[22]

På grund af de mange forsøg på at trænge ind og det stadig større antal måder, hackere kan trænge ind på, mener O'Keeffe og andre eksperter, at det er bedre for sikkerhedschefer at forestille sig, at der allerede er sket brud på netværkssikkerheden. "Alle sikkerhedseksperter skal erkende, at deres netværk måske allerede er kompromitteret. De ved det bare ikke endnu ", siger O'Keeffe.

O'Keeffe har analyseret it-sikkerhedsprotokoller hos over 50 små og store virksomheder, og han siger, at de alle har svagheder, der kan give en hacker adgang til netværket via en af printerne, kameraerne, mobilenhederne eller andre slutpunkter, der er tilsluttet netværket.

Derfor beskytter man et netværk ved at give it-medarbejderne værktøjer til at opdage angreb og beskytte slutpunkter, som er de adgangspunkter, der er nemme at overse, og som en beslutsom fjende kan udnytte, hvis sikkerheden ikke er i orden. O'Keeffe understreger, at hvis nogen skulle trænge ind, så er det vigtigt at have en solid gendannelsesplan, så skaden hurtigt kan udbedres.

Daniel Kalai har stiftet flere it-servicevirksomheder, deriblandt it-sikkerhedsvirksomheden Shieldly, der har fokus på private og små virksomheder. Han er enig med Albright og O'Keeffe om, at man bør fokusere på at beskytte et netværks yderområder og slutpunkter.[23] Men han mener, at man lægger for stor vægt på gendannelse i stedet for forebyggelse. Han er ikke enig i, at et kompromitteret netværk er uundgåeligt i den moderne digitale tidsalder.

"Internetsikkerhed handlede tidligere om forebyggelse", siger Kalai. "Men nu handler det i høj grad om udbedring. Det er trist at se på, hvad der sker, når folk mister troen på forebyggelsesværktøjer. Men man kan gøre meget for at forhindre et angreb."

Prisen for fiasko

Bedre brug af enheder, standarder og protokoller, når det gælder sikkerhed, ville bestemt forbedre resultaterne for dem, der iværksætter forsvarsprogrammer til internetsikkerhed, men de reelle data viser, at der er stor forskel på planlægning og udførelse.[24] Og selvom organisationer er truet af de samme ting, så er problemet større for små virksomheder, fordi de ikke har tid og penge og de samme ressourcer til at investere i sikkerhed ligesom de større organisationer.[25]

Det er grunden til, at alle, der har ansvar for en virksomheds it-sikkerhed, skal mindes om, hvad der står på spil: Et potentielt milliontab, et katastrofalt fald i troværdigheden og kundernes tillid samt sagsanlæg og enorme problemer pga. afbrydelser i driften.

Ifølge en rapport fra Ponemon Institute, der er en uafhængig forskningsgruppe inden for informationssikkerhed, kostede et gennemsnitligt dataindbrud 3,62 mio. $ i 2017.[26] Forskerne har interviewet personer i 419 virksomheder i 13 lande og konkluderet, at hver enkelt mistet eller stjålet dokument i gennemsnit koster 141 $. Dette beløb kan hurtigt blive stort, fordi dette sker så tit. Konklusionen på undersøgelsen var faktisk, at størrelsen på det gennemsnitlige brud steg med 1,8 procent i 2017 i forhold til året før.

Alle de virksomheder, der gav deres oplysninger til Ponemon, rapporterede et brud på grund af et ondsindet eller kriminelt angreb, en systemfejl eller en menneskelig fejl, hvor antallet af kompromitterede poster i hver hændelse lå mellem 2.600 til lige under 100.000. Undersøgelsens respondenter brugte i gennemsnit mere end to måneder på at identificere og inddæmme bruddet.

Malware bliver klogere

Jonathan Griffin er seniorforsker i sikkerhed hos HP Labs og udtaler, at han ser flere højprofilerede brud, der giver et "chokerende omfang af skader og ødelæggelse", herunder NotPetya fra 2017, der ramte virksomheder i USA og i hele Europa, og hvis primære formål tilsyneladende kun var at udrette skade.[27] Ligesom med andre vellykkede angreb fandtes der et forsvar mod WannaCry, før angrebet fandt sted. Desværre viste det sig, at mange organisationer, både store og små, ikke havde installeret de simple softwarerettelser, der kunne have forhindret angrebet.

Men vellykkede hacks er ikke blot et tegn på, at sikkerheden ikke er i orden.
Hos HP's malwarelaboratorium har Griffin og hans team bemærket, at malware er blevet mere omfattende og kompleks i de seneste tre år. Programmerne er blevet betydelig mere effektive og minder om kommerciel software, dvs. at de er godt designet og er med høj kvalitet.
Griffin siger, at kriminelle og statsstøttede hackere er velorganiserede og meget kompetente teknikere, der hele tiden forbedrer deres håndværk og benytter sig af nye værktøjer, f.eks. maskinlæring, der giver systemer mulighed for at lære af erfaring og blive bedre uden at være programmeret til dette.

> Kombinationen af den stadig større kompleksitet og mangelfuld it-sikkerhed forstærker risikoen i virksomhedernes netværk.

Kombinationen af den stadig større kompleksitet og mangelfuld it-sikkerhed forstærker risikoen i virksomhedernes netværk. Ifølge Griffin er der heldigvis mange dataloger og -teknikere i hele verden, der arbejder på at forbedre forsvarsmulighederne. Og eksperter siger, at organisationerne omsider er ved at indse, at installationen af firewall og antivirussoftware blot er de første skridt på vejen mod et effektiv program, hvor forsvarsmekanismer i flere lag og intrusion detection også er en vigtig del.

Afsnit 2:

Tænk ligesom da Vinci: Der kræves mere kunstnerisk håndelag inden for it-sikkerhed

Nuværende og fremtidige it-trusler kræver en blanding af kunst og videnskab.

Begrebet "renæssancemenneske" – dvs. en person, som er dygtig til flere ting – blev udtænkt med Leonardo da Vinci for øje. Skaberen af mesterværker såsom Den sidste nadver og Mona Lisa var både opfinder og kunstner.
Da Vinci arbejdede med våbenteknologi i næsten to årtier og forstærkede Milanos forsvar, samtidig med at han også opfandt og forbedrede våben. I hele sit liv opfandt og forbedrede han teknikker til at bygge broer og forbedrede maskinkomponenter som f.eks. snekkehjul og svinghjul. Han var ekspert i hydraulik og designede endda en fjederdrevet bil.

It-sikkerhedsbranchen kunne lære en hel del af dette geni. Nuværende og fremtidige it-trusler kræver en blanding af kunstnerisk håndelag og videnskab – især når det gælder design.

De personer, der er ansvarlige for en virksomheds informationssikkerhed, skal se på alle de fysiske og digitale aktiver, der er knyttet til organisationen, hvor de er placeret på netværket, hvordan de tilsluttes, og hvordan de vedrører andre aktiver. En endnu vigtigere ting er medarbejdernes brug af slutpunkter som f.eks. smartphones, printere og bærbare computere til at udføre arbejdet, da dette skal være et centralt led, når man planlægger sikkerhed og arkitektur.

Når alt kommer til alt, er det bedste forsvar at beskytte netværket, uden at brugerne overhovedet ved, at det er der. Her er et nyttigt mantra, som it-sikkerhedschefer skal huske på: Brug intelligent teknologi, vær usynlig, og vær hele tiden på forkant med truslen.

Aktiv overvågning er altafgørende

Allen Kent er it-sikkerhedskonsulent og ansat hos NAES Corporation, som tilbyder en række serviceydelser til brancher lige fra energisektoren til papirproducenter.[28] Kent undersøger kraftværker flere gange om året og leder efter huller i it-sikkerheden. Han bliver tilkaldt i forbindelse med kontrol af energiselskaber samt ejere af transmissionssystemer og -distributører, så de er klar til at få kontrolleret deres it-forsvar, der er påkrævet ifølge myndighederne.

Denne myndighedskontrol sker hvert tredje til sjette år, alt efter hvor omfattende et it-sikkerhedsbrud i en virksomhed vil være for elnettets samlede stabilitet. Sært nok er den generelle opfattelse, at de fleste generatorer ikke vil have den store betydning. Et sikkerhedsbrud vil få store konsekvenser, hvis der er et systemisk problem i det såkaldte kontrolcenter for afbalancering, der håndterer variation i elforsyningen og efterspørgslen i flere områder og i hele landet.

Før Kent kom til at arbejde med den kritiske infrastruktur til elproduktion, arbejdede han med it-sikkerhed i banksektoren, så han har i årevis udtænkt metoder til at eliminere trusler fra organiserede forbryderorganisationer og statsstøttede grupper. Han siger, at selvom elselskaberne har en hel del arbejde, de skal nå, før de overholder de myndighedernes krav, så er energisektorens it-sikkerhed faktisk OK i forhold til den finansielle sektors. "Den er ikke fantastisk, men OK", udtaler han.

En af Kents største udfordringer er at få de ansvarlige til at indse, at der ikke findes nogen effektiv it-sikkerhedsløsning, som man hurtigt kan installere og derefter tro, at alt er i skønneste orden. "Forsvarssystemet skal hele tiden overvåges", siger han. "Men uanset hvilken branche der er tale om, så vil de fleste små virksomheder ikke betale andre for at gøre dette. Det er en løbende udgift uden afkast – lige indtil der sker et brud på sikkerheden, der koster langt mere end det honorar, som den pågældende leverandør skulle have haft."

Kent fortæller virksomheder, at det første led i deres it-sikkerhedsprogram er fire ting: Installation af en firewall, der er konfigureret til at virke efter hensigten. Opsætning af systemer, der overvåger og fjerner skadeligt eller mistænkeligt indhold fra e-mail og browsere. Isolering af beskyttede aktiver fra dem, der ikke kræver det samme sikkerhedsniveau (hos et elselskab skal computere til drift af anlægget for eksempel isoleres fra dem, der bruges til virksomhedsdriften). Oprettelse af protokoller, ansættelse af personale og anskaffelse af software, så det hele kan overvåges aktivt. Denne standardmodel for it-sikkerhed kaldes et grænseforsvar: Det skaber digitale vægge og systemer til registrering af indtrængen, der forhindrer uvedkommende i at få adgang.

Men nu findes der nye våben, der giver it-sikkerhedschefer mulighed for at være endnu mere offensive. For ikke så lang tid siden mente eksperter, at der ikke fandtes en forebyggelsesstrategi mod alle de nye trusler på internettet. Men de nyeste værktøjer til automatisk registrering begynder at overvåge, hvordan netværket fungerer for at finde ud af, hvordan data normalt sendes på netværket, så de kan opdage og forhindre sikkerhedsbrud, der kan medføre skader. En tilsyneladende lille hændelse, hvor en bærbar computer f.eks. sender adskillige gigabyte data ud af et netværk, der normalt sender hundredvis af megabyte, kan udløse en alarm.

De fire søjler inden for it-sikkerhed til netværk:

01 Installér en firewall

02 Overvåg og fjern skadeligt eller mistænkeligt indhold

03 Isoler beskyttede aktiver

04 Udarbejd protokoller

"Du er nødt til at kunne registrere, reagere og derefter genoprette netværk og enheder hurtigt og i stort omfang."

VALI ALI
HP Fellow and Chief Technologist

Det er ikke kun vinteren, der kræver ekstra beskyttelse

"Vi er nødt til at bygge enheder med flere forsvarsniveauer", udtaler Albright fra HP. "Det kalder vi forsvar i dybden. Da du ikke kan beskytte dig mod alt, skal du være i stand til at holde øje med og opdage unormal adfærd på enheden, som kan være tegn på et angreb."

HP Fellow og Chief Technologist Vali Ali går et skridt videre og siger, at sikkerheds- og registreringsfunktioner skal være indbygget enheder på netværket. De skal ikke tilføjes bagefter.[29] I de seneste år er der sket meget inden for sikkerhedsintelligens, blandt andet i form af software, der registrerer trusler, stopper dem og sletter malwaren på maskinen automatisk. Men før den kan fungere optimalt, skal den være indbygget, så den er tydelig for brugeren, og være fleksibel nok til at modstå flere angreb.

Derudover skal it-køb også kun foretages efter nøje overvejelse, så man kan finde det udstyr, der både kan klare opgaven samt beskytte brugere og data. "Ethvert køb af en enhed er en sikkerhedsmæssig beslutning", siger Ali og tilføjer, at sikkerhed er en kombination af teknologi, kendskab, proces og ledelse.

Netværk og enheder skal ikke kun have intelligente registrerings-, respons- og læringsfunktioner. De skal også være modstandsdygtige, så de kan gendannes hurtigt efter sikkerhedsbrud. "Du vil blive udsat for et angreb", siger Ali. "Du er nødt til at kunne registrere, reagere og derefter genoprette netværk og enheder hurtigt og i stort omfang."

Fare ved netværkets kant

Visse store virksomheder har ressourcer til at lade beskyttelsen nå helt ud til periferien af deres netværk. Men mange mellemstore og store virksomheder har ikke beskyttet deres smartphones, scannere, printere og IoT-enheder.[30] HP's Albright siger, at hendes samtaler med kunderne ofte afslører en uventet mangel på bekymring, når det gælder beskyttelsen af slutpunkterne i komplekse netværk.

"Det overrasker mig, at mange kunder er meget bevidste om, at deres pc'er, servere og netværksenheder er i fare, mens de til gengæld overhovedet ikke bekymrer sig om printere eller andre IoT-enheder", siger hun. "Det er lige præcis her, at vi forsøger at lære folk mere og fortælle, at hvis man har et slutpunkt på sit netværk, der er udsat eller ubeskyttet, så kan det medføre en risiko for hele infrastrukturen."

Først skal it-afdelingerne have styr på det grundlæggende: 1) De skal udvikle og overholde strenge sikkerhedsprotokoller, herunder krav om,at fabriksindstillede adgangskoder og adgangskoder til vedligeholdelse med det samme ændres på alle enheder. 2) De skal have rettidige tidsplaner for sikkerhedsrettelser og -opdateringer for alle enheder i netværk. 3) De skal konfigurere automatisk opdatering eller hasteopdatering af operativsystemer og programmer samt firewalls og antivirusdefinitioner. Virksomhederne skal desuden ajourføre deres medarbejderjournaler og hurtigt fjerne adgangsprivilegier for de medarbejdere, der ikke er ansat i virksomheden længere.

Ali siger, at det også er vigtigt at give folk en forståelse for, hvordan det moderne kontor udvikler sig lige nu. Medarbejdere forventer i stigende grad, at de kan arbejde hvor som helst og når som helst, og arbejde og fritid blandes ofte sammen eller bytter plads. Arbejde kan udføres på stranden, mens der kan være happy hour på arbejdet. "Fremtidens kontor har åbne grænser", siger Ali. "Det er en type miljø, der kører døgnet rundt, hele året, og hvor dit privatliv og arbejdsliv er flettet sammen Netværksinfrastruktur, -enheder og -teknologier skal være helt opdateret for at kunne holde trit med denne forandring.

Sikkerhedsforskeren Griffin har lagt mærke til, at it-sikkerhedseksperter kæmper i en krig, hvor de er nødt til at vinde hver eneste dag, hvorimod fjenden kun skal have heldet med sig én gang. Han anbefaler syv retningslinjer, der på længere sigt vil forbedre it-sikkerheden:

01 Udarbejd nemme processer, der ikke er for komplekse eller virker som magi.

02 Giv brugere enkel, ensartet rådgivning.

03 Brug tofaktorgodkendelse, når det er muligt, da der er mange problemer med adgangskoder og politik for virksomhedsadgangskoder.

04 Brug ikke kun prisen som beslutningsgrundlag. Omdan gode sikkerhedspolitikker til gode sikkerhedsprodukter til gode sikkerhedsbeslutninger.

05 Nøjes ikke med et "sikkerhedsshow" og afkrydsning af punkter, når du udarbejder din virksomheds sikkerhedspolitikker. Sørg for, at de sikkerhedsfunktioner, som du betaler for, rent faktisk gør din organisation sikker.

06 Opret flere meningsfulde rapporter ved at få analytiske værktøjer, der ikke kun viser, hvor mange angreb og hvor meget virus dit sikkerhedssystem har stoppet på en måned, men også hvor mange af disse, der var nye og unikke.

07 IoT-enhedsproducenter bør implementere sikkerhed i deres produkter fra starten af og sørge for, at de "som standard er sikre".

Vigtigheden af at uddanne medarbejdere

Den moderne nedrivning af kontorvæggene forværrer et problem, der altid har været centralt for sikkerhedshuller: menneskelig adfærd. Medarbejdere springer tunge sikkerhedsprotokoller over for at være produktive og er ofte ikke klar over, at deres onlineadfærd er farlig. Det er grunden til, at små utilsigtede handlinger med dårlig "onlinehygiejne" hyppigt er kilden til netværksfejl, tyveri af immateriel ejendom eller følsomme kundedata og slutpunkter, der bliver kidnappet af et botnet. "Der er altid en eller anden, der klikker på et ondsindet link i en e-mail", siger Albright.

En velanset virksomhed med speciale i anti-malware rapporterer, at kun 3 procent af den malware, de ser, går efter tekniske fejl.[31] Det betyder, at 97 procent af disse hackere bruger social engineering til at få intetanende ofre til at klikke på et link i en phishingmail eller afsløre følsomme data som f.eks. adgangskode og bankkontinumre.

Derfor er uddannelsesinitiativer til udvikling og opretholdelse af stærke protokoller og procedurer til informationssikkerhed vigtige, både for medarbejdere i it-afdelingen og medarbejdere i andre afdelinger. De vil minimere skødesløs adfærd hos slutbrugerne, der skaber meget store sikkerhedsrisici.

Vigtige punkter ved uddannelse af medarbejdere, der ikke har med it at gøre:

Brug ikke den samme adgangskode på flere personlige og arbejdsrelaterede websteder.

- Efterlad ikke følsomt materiale på printere.
- Lås computeren og enhederne, når de ikke er i brug.
- Brug skærme til enhederne, der forhindrer andre i at se oplysninger på computeren.
- Klik for alt i verden ikke på links uden at tænke over det.

Hvordan tager de bedste systemers designere, arkitekter og teknikere højde for menneskelig adfærd, når de skal forbedre, hvordan organisationer beskytter deres netværk og aktiver?

Fremtidens våben til nutidens trusler

Ali og sikkerhedsforskeren Griffin peger på en række af HP's nyskabelser, der nu er tilgængelige for offentligheden, og som ikke mindsker brugernes produktivitet, så der er mindre sandsynlighed for, at medarbejdere ignorerer eller slår dem fra.

Et af disse fremskridt er HP Secure, der er en programpakke til beskyttelse af pc'er, der omfatter Sure View, Sure Click og Sure Start.

HP Sure View er en integreret skærm til beskyttelse af indhold på pc'er, der forhindrer andre i at se data på medarbejdernes skærme. "Dette er en rigtig god sikkerhedsfunktion", siger Griffin. "Den er nem at bruge, medarbejderne ved, at den er der, og de ved, hvad den gør".

HP Sure Click er hardwarehåndhævet sikkerhedsforanstaltning til browsere, der isolerer malware på en virtuel maskine, så den ikke inficerer systemet. "Hvor tit har du ikke klikket på et link og øjeblikkeligt sagt "Åh, nej, jeg skulle ikke have klikket?", siger Ali. "Sure Click sørger for, at malware ikke kan se noget på din maskine. Skulle der ved et uheld blive downloadet malware, kan brugerne blot lukke fanen, og så er den væk. Det er helt suverænt, fordi vi ikke beder brugerne om at ændre deres adfærd for at gøre det mere sikkert at surfe".

Med denne type it-sikkerhed, hvor brugerne fjernes fra ligningen, elimineres den menneskelige faktor i forbindelse med sikkerhedsbrud på netværk.

Det indbyggede **HP Sure View**-sikkerhedsfilter er valgfrit og skal konfigureres ved købet. Kun tilgængelig på udvalgte HP-notebooks.

HP Sure Click fås til udvalgte HP-platforme og understøtter Microsoft® Internet Explorer og Chromium™. Her kan du se alle kompatible platforme, når de bliver tilgængelige.

HP Sure Start Gen4 fås til HP Elite- og HP Pro 600-produkter med 8. generations Intel®- eller AMD-processorer.

HP Sure Start er et helt nyt forsvar mod malware, der analyserer BIOS-firmware, som er den mest grundlæggende del af en computers operativsystem – et område, der stadig bliver mere udsat for angreb, fordi det er meget vanskeligt at opdage indtrængen her. Uden et ordentligt forsvar er malware, der er installeret i BIOS, usynligt, og det giver en angriber mulighed for at eksistere permanent på netværket. Ifølge Verizons Data Breach Investigations Report fra 2016 benyttes denne fremgangsmåde endnu oftere af angribere. Analytikerne så en stigning på 132 procent i forhold til hændelser mod notebooks og stationære computere i det forrige år.[32]

HP Sure Start forhindrer, at bedragere kan opholde sig i et netværks BIOS. Når pc'en starter, bekræfter den integrerede funktion, at BIOS er ren. I modsat fald gendanner HP Sure Start automatisk koden til en ren version, uden at brugeren eller it-afdelingen skal gøre noget. "Den er sikker som standard", siger Ali.

Afsnit 3:

Vi ser nærmere på: Maskinlæring og kunstig intelligens

Vores digitale beskyttelse af nærmiljøet er ved at få noget hjælp fra kunstig intelligens via maskinlæring.

Selv om de bedste af de nuværende fremgangsmåder til internetforsvar omfatter lagdelt teknologi, biometriske logons og netværksovervågning samt en god uddannelse af medarbejdere i onlinehygiejne, begynder vores digitale beskyttelse af nærmiljøet at få noget hjælp fra kunstig intelligens via maskinlæring.

Et af HP's fremskridt kan beskytte disse sårbare, netværkstilsluttede slutpunktsprintere. HP Connection Inspector er udviklet hos HP Labs og er tilgængelig nu. Det er en intelligent, integreret sikkerhedsfunktion, der lærer, hvordan en printers normale netværksadfærd ser ud og derefter registrerer mistænkelige ændringer. Når den registrerer nogle usædvanlige udgående data, giver den administratorerne besked, lukker den mistænkelige kommunikation ned og gennemtvinger derefter en selvhelbredende genstart, der fjerner malwaren og stoppe angrebet.

Netop denne udvikling gør Kent fra NAES til en forsigtig optimist. Han håber, at teknikere en dag kan slutte en enhed til netværket, der holder øje med trusler i datakommunikationen og øjeblikkeligt stopper dataudvekslingen i tilfælde af sikkerhedsbrud og derefter undersøger angrebet for at konkludere, hvordan et lignende vil se ud, når det starter. "En boks med kunstig intelligens, der overvåger alt og stopper en trussel automatisk, når den viser sig, ville være fedt", siger han.

Sådan bliver IoT-enheder til en del af forsvaret

Integrering af processorer og internetadgang til termostater, bevægelsessensorer, belysning og andre systemer betyder, at en kontorbygning selv kan finde væsentlige energibesparelser baseret på tilstedeværelse, klokkeslæt og endda vejret.[33] En vindturbine fortæller de ansvarlige, at tandhjulene i nacellen vibrerer for meget og skal efterses[34]. En kommerciel jetmotor og flycomputer arbejder sammen for at lave ændringer i sidste øjeblik, reducerer brændstofforbruget og forkorter en rute.[35]

Disse smarte enheder kommer altså ind i vores hjem i form af intelligente termostater, intelligente køleskabe, intelligente elpærer og digitale assistenter, der drives af kunstig intelligens. I fremtiden vil vi også have intelligente proteser

og nethindeimplantater, der vil blive indlejret med meget små processorer og have internetforbindelse. Men hvad sker der, hvis hackere går efter dem?

"Forestil dig et nethindeimplantat eller en amputeret person med et 3D-printet ben, og forestil dig, at den protese rammes af et firmwareangreb eller inficeres med ransomware", siger HP's Ali. "Hvordan ville det se ud? Hvad ville folk gøre, hvis de pludselig mistede evnen til at se og fik meddelelsen "Betal, eller du mister synet"?

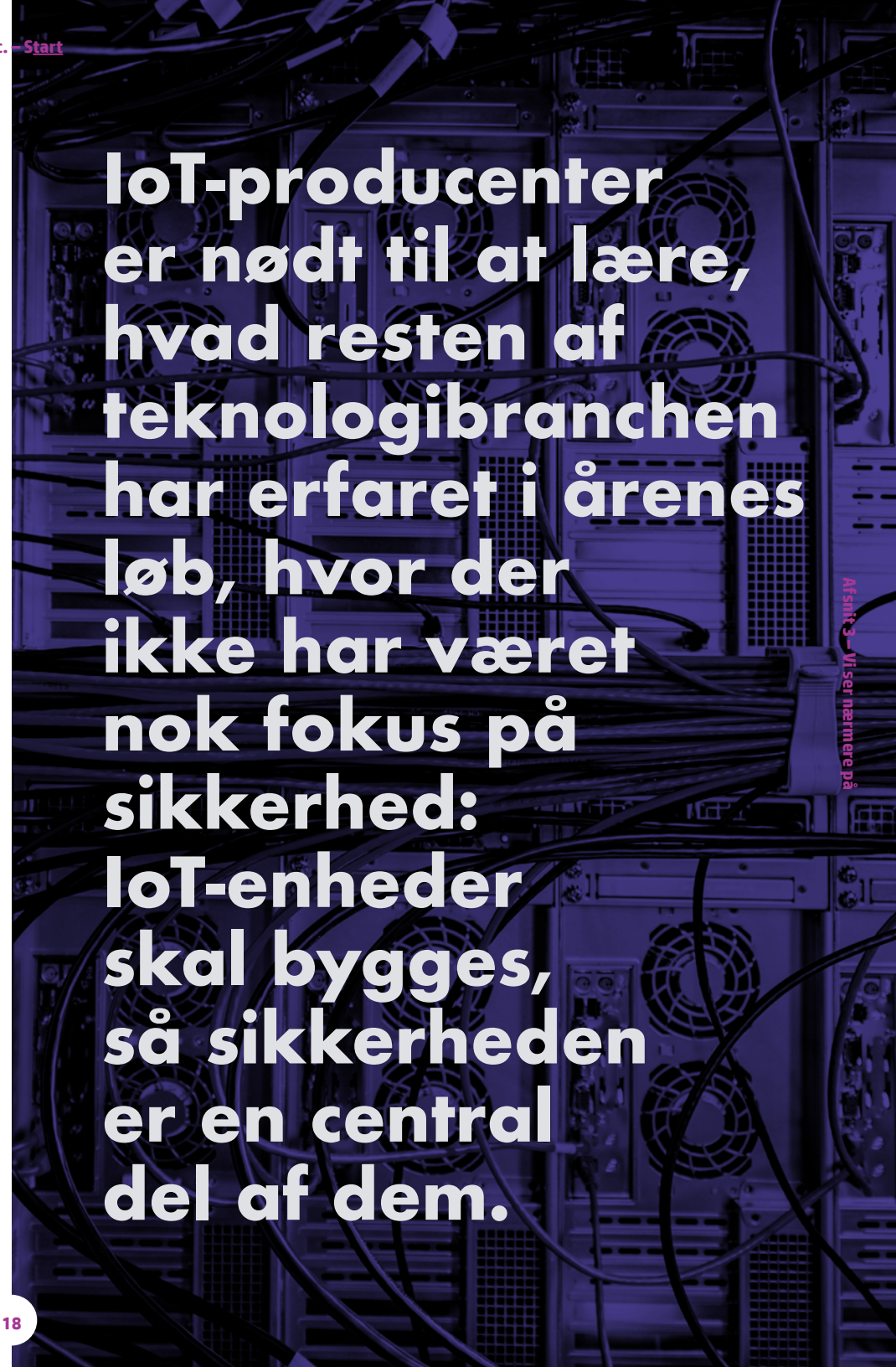
Det er her, fleksibilitet kommer ind i billedet, så en inficeret maskine hurtigt kan fjerne softwaren og komme online igen i en ren tilstand. "Når et nethindeimplantant bliver inficeret af malware eller ransomware, skal du bare blinke med øjnene. Så forsvinder malwaren, og du kan se igen", siger Ali.

For at kunne gøre dette, siger Griffin, er IoT-producenter nødt til at lære, hvad resten af teknologibranchen har erfaret i årenes løb, når der ikke har været fokus nok på sikkerhed: Sikkerheden skal være en central del af IoT-enheder, når de fremstilles. Det vil betyde, at hvis en intelligent elpære bliver ramt af malware, så bør den kunne slukke lyset, genstarte, slette den fremmede kode og lyse igen efter nogle blink.

Brugervenlighed beskytter mod skadelig adfærd

"Jeg vil ikke acceptere, at jeg skal sætte en nøgle i min dør og vente på en sms-besked, hvor jeg skal bekræfte, at det er mig, der prøver at åbne døren", siger Griffin "Det må ikke virke forstyrrende i min hverdag."

For at håndtere denne problemstilling, der har været kendt længe, har teknikere i årevis arbejdet på at forbedre loginmetoder, blandet andet med ansigtsgenkendelse baseret på computersyn og biometriske udfordringer med fingeraftryk eller nethindescanning, der så småt er ved at erstatte de gamle alfanumeriske adgangskoder.[36]



"Det er et våbenkapløb, og det er altid svært at vide, hvor angriberne slår til næste gang."

JONATHAN GRIFFIN,
Senior Security Researcher
for HP Labs

En anden løsning er HP's WorkWise-teknologi, som er en gratis app, der kan hentes i Google Play, og som opretter en sikker kryptografisk forbindelse mellem en medarbejders smartphone og computer. Med denne forbindelse kan computeren se, om brugeren har forladt computeren, hvilket automatisk låser computeren, så andre ikke har adgang. Når brugeren kommer tilbage, genkender computeren brugeren og logger vedkommende på, uden at det er nødvendigt at bruge en adgangskode. Denne teknologi er godt eksempel på minimal forstyrrelse i hverdagen, fordi brugerne beskyttes uden at blive bedt om at gøre mere.

"Der findes to typer teknologi", siger Ali. "Den type, som folk vil bruge, og den besværlige type, de er nødt til at bruge". Hvis det er den besværlige sikkerhed, de er nødt til at bruge, finder de på et eller andet tidspunkt en måde at omgå den på".

Maskinlæring er et tveægget sværd

De dage, hvor malwarescanning var hovedværktøjet mod angriberne, er forbi.[37] Anti-malwaresoftware skal være opdateret med kendt, skadelig kode for at vide, hvad den skal kigge efter. Dette nytter ikke, når der lægges nye skadelige koder på internettet, hvilket sker med en hastighed, der overrasker forskerne.

På forsvarets side kan data og maskinlæring efterhånden bruges til automatiserede netværksanalyser, der analyserer strømmen af data i hele virksomhedens netværk og holder øje med unormale ting. Sådanne computerfunktioner vil f.eks. en dag kunne opdage store stigninger i processoraktiviteten, der kan være et tegn på et nyt problem. På angrebets side kan maskinlæring selvfølgelig også bruges til at undersøge, scanne og rense netværket.

Griffin fra HP siger, at maskinlæring og andre former for kunstig intelligens allerede giver forsvaret en fordel. Han advarer dog om, at værktøjer som maskinlæring ikke er et universalmiddel. Faktisk vil maskinlæring sandsynligvis blive en ny flanke, som kan angribes af hackere, der leder efter svagheder i maskinlæringsbasede beskyttelsesforanstaltninger og selv anvender maskinlæring/kunstig intelligens til at designe billigere og mere effektive angreb. "Det er et våbenkapløb, og det er altid svært at vide, hvor angriberne slår til næste gang", siger han.

Vil kunstig intelligens løse problemet med it-sikkerhed eller gøre det værre?

På længere sigt vil de avancerede algoritmer i hjertet af problemløsning med maskinlæring udvikle sig til mere robuste systemer med kunstig intelligens. De angribere, der har ressourcerne til rådighed, vil bruge kunstig intelligens til at teste og angribe netværk. Den avancerede teknologi vil give dem mulighed for at forbedre adfærdsbaserede tricks, der gør det muligt at skelne mellem malwareangreb og legitime e-mails og websites. Både angrebet og forsvaret vil anvende kunstig intelligens til at omdirigere netværksdata under DDoS-angreb på en intelligent måde for at forstærke eller afhjælpe skaden.

"Vi kommer til at leve i en verden med intelligente angreb, der er baseret på kunstig intelligens", siger Ali. "Det er måske allerede sket, men systemet er intelligent nok til, at ingen har opdaget det".

I fremtiden skal teknikere fremme de dynamiske læringsmuligheder ved kunstig intelligens i en sådan grad, at forsvarets systemer kan bruge historiske data og tendenser til at forudse angreb, eliminere eller inddæmme dem og måske endda opspore de kriminelle aktører.

Nu begynder forudseende producenter dog at producere de første enheder, der ligner dem, som Kent fra NAES drømmer om: Kunstig intelligens i en boks. Det første skridt er at gøre sikkerhed til en central del af produkterne helt fra begyndelsen af designprocessen.

Den evige kampe mellem det gode og det onde skal vindes

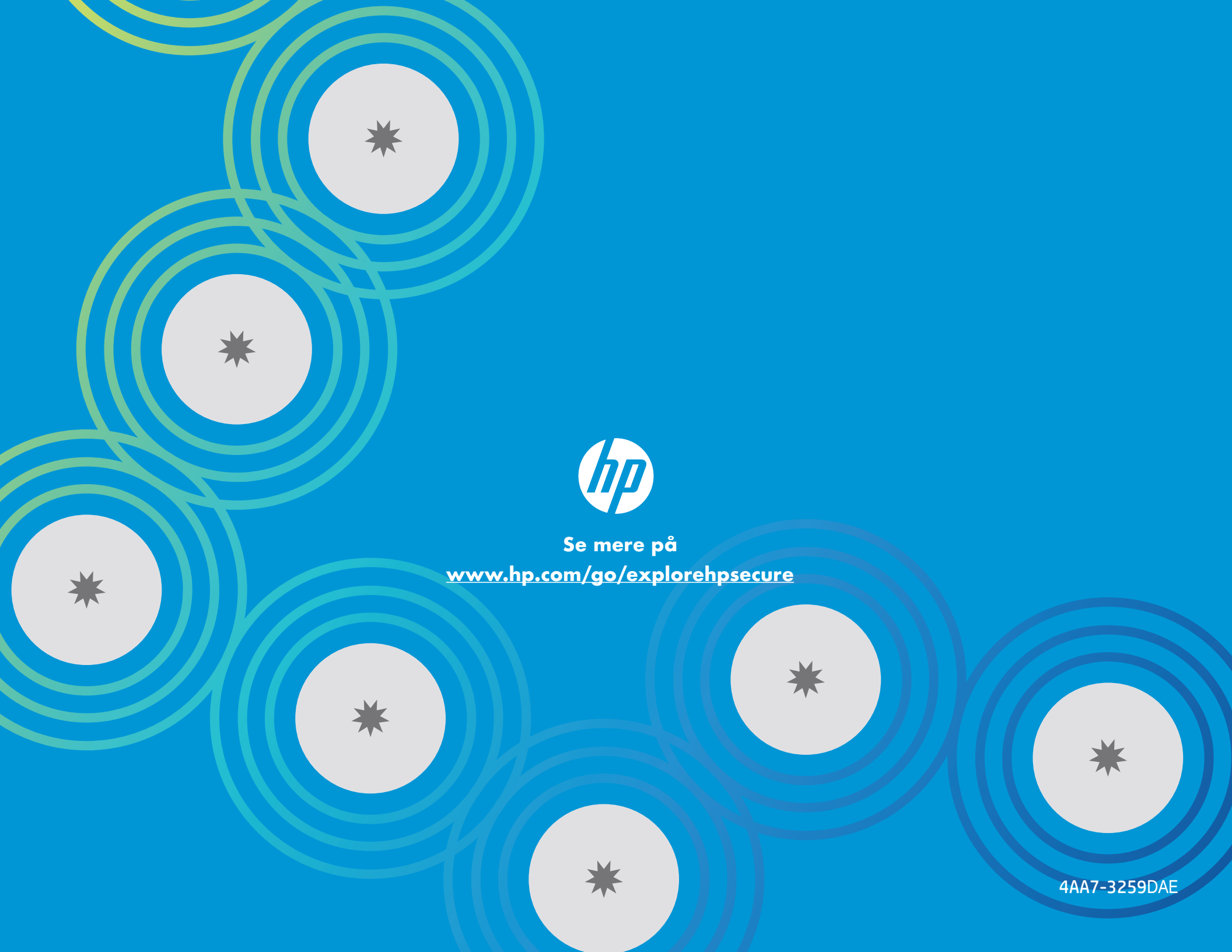
Internetkrigen mellem de gode og de onde raser, og resultatet er ikke det samme i alle brancher. Både kriminelle og politiske elementer gør, hvad de kan for at filtrere og forstyrre netværk, og der står utroligt meget på spil. Truslerne kan ikke ignoreres.

> Der udkæmpes hele tiden en kamp mellem de gode og de onde. Vi er de gode, og vi må ikke tabe denne kamp. Det må ikke ske. Hos HP er vi forpligtet til følgende: Denne kamp vil vi ikke tabe".

Beskyttelsen af de digitale systemer, der styrer kritisk infrastruktur og offentlige myndigheder samt både store og små virksomheder, er altafgørende for vores hverdag, folks levebrød og samfundet som helhed. "Vi tror, at der er en skræmmende verden derude, men der findes også gode mennesker", siger Ali fra HP. "Der udkæmpes hele tiden en kamp mellem de gode og de onde. Vi er de gode, og vi må ikke tabe denne kamp. Det må ikke ske. Hos HP er vi forpligtet til følgende: Denne kamp vil vi ikke tabe".

Slutnoter

1. Robotics Business Review, "Robot Investments Weekly: AI, Industrial Automation, Mobility Market Drive Spending", https://www.roboticsbusinessreview.com/financial/robot-investments-weekly-ai-industrial-automation-mobility-market-drive-spending/ (åbnet 26. feb. 2018)
2. TechEmergence, "Machine Learning Drug Discovery Applications – Pfizer, Roche, GSK, and More", https://www.techemergence.com/machine-learning-drug-discovery-applications-pfizer-roche-gsk/ (åbnet 26. februar 2018)
3. Popular Mechanics, "The Surgeon Will Skype You Now", https://www.popularmechanics.com/science/health/a19208/the-surgeon-will-skype-you-now/ (åbnet 26. februar 2018)
4. CFO, "Cyber Attacks Can Cause Major Stock Drops", http://ww2.cfo.com/cyber-security-technology/2017/04/cyber-attacks-stock-drops/ (åbnet 26. februar 2018)
5. Kaspersky, "Cyberthreat Real-Time Map: Local infections in the last week", https://cybermap.kaspersky.com/stats/ (åbnet 26. februar 2018)
6. Anti-Phishing Working Group, "Global Phishing Survey" https://apwg.org/resources/apwg-reports/domain-use-and-trends
7. G DATA Security Blog, "Malware Trends 2017", https://www.gdatasoftware.com/blog/2017/04/29666-malware-trends-2017
8. Digital Attack Map, "What is a DDoS Attack?" http://www.digitalattackmap.com/understanding-ddos/
9. Digital Attack Map, "Top Daily DDoS Attacks Worldwide," http://www.digitalattackmap.com/
10. U.S. Department of Defense, "'Terabyte of Death' Cyberattack Against DoD Looms, DISA Director Warns", https://www.defense.gov/News/Article/Article/1414146/
11. HP, "HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack", http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676
12. Greenfield Daily Reporter, "Hospital Falls Victim To Hacker Attack; No Patient Records Compromised", http://www.greenfieldreporter.com/2018/01/12/hospital-falls-victim-to-hacker-attack-no-patient-records-compromised-officials-said/
13. Black Hills Pioneer, "Belle Fourche City Servers Hacked", http://www.bhpioneer.com/local_news/belle-fourche-city-servers-hacked/article_7254ad36-f576-11e7-8ed7-e31c3ee0da87.html
14. Columbia Daily Herald, "MCPS Experiences Cyber Attack", http://www.columbiadailyherald.com/news/20180105/mcps-experiences-cyber-attack
15. Bloomberg Technology, "It Can't Be True.' Inside the Semiconductor Industry's Meltdown", https://www.bloomberg.com/news/articles/2018-01-08/-it-can-t-be-true-inside-the-semiconductor-industry-s-meltdown
16. The Economic Times of India, "3.2 Million Debit Cards Compromised; SBI, HDFC Bank, ICICI, YES Bank and Axis Worst Hit", (Paywall) https://economictimes.indiatimes.com/industry/banking/finance/banking/3-2-million-debit-cards-compromised-sbi-hdfc-bank-icici-yes-bank-and-axis-worst-hit/articleshow/54945561.cms
17. CNBC, "Virtual Extortion a Big Business for Cyber Criminals", https://www.cnbc.com/2016/02/17/ransomware-is-targeting-us-companies-of-all-sizes.html
18. Cybersecurity Ventures, "Cybercrime Report", https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
19. Telefoninterview med Jason O'Keeffe, HP (December 14, 2017)
20. Telefoninterview med Shivaun Albright, HP (December 15, 2017)
21. CoinDesk, "Botnet Infects Half a Million Servers to Mine Thousands of Monero", https://www.coindesk.com/botnet-infects-half-million-servers-mine-thousands-monero/
22. Telefoninterview med Daniel Kalai, Shieldly (January 10, 2018)
23. Financial Times, "Essential' services face fines for poor cyber security", (Paywall) https://www.ft.com/content/f2faf8cc-7b79-11e7-ab01-a13271d1ee9c
24. Houston Chronicle, "Consequences of Poor Security in a Company", http://smallbusiness.chron.com/consequences-poor-security-company-70227.html
25. IBM and Ponemon Institute, "2017 Ponemon Cost of Data Breach Study", https://www.ibm.com/security/data-breach
26. Telefoninterview med Jonathan Griffin, HP (21. December 2017)
27. Telefoninterview med Allen Kent, NAES (15. January 2018)
28. Telefoninterview med Vali Ali, HP (15. December 2017)
29. Keeper Security, "2017 State of Cybersecurity in Small & Medium-sized Businesses", https://keepersecurity.com/2017-State-Cybersecurity-Small-Medium-Businesses-SMB.html
30. Digital Guardian, "Social-Engineering Attacks: Common Techniques & How to Prevent an Attack", https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack
31. Verizon, "2016 Data Breach Investigations Report", http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf
32. Intel, "Reduce Energy Costs and Carbon Footprint with Smart Building Management", https://www.intel.com/content/dam/www/public/us/en/documents/solution-briefs/iot-ecs-tatung-reduce-carbon-footprint-solution-brief.pdf
33. Industrial Internet Consortium, "The Benefits of IoT Analytics for Renewable Energy", https://www.iiconsortium.org/case-studies/ParStream_Envision_Energy_Case_Study.pdf
34. Aviation Week, "Internet Of Aircraft Things: An Industry Set To Be Transformed", http://aviationweek.com/connected-aerospace/internet-aircraft-things-industry-set-be-transformed
35. Global Cyber Alliance, "How Biometrics Can Replace Passwords", https://www.globalcyberalliance.org/how-biometrics-can-replace-passwords.html
36. Wall Street Journal, "The Limits of Antivirus Software", (Paywall) https://www.wsj.com/articles/the-limits-of-antivirus-software-1505700000



Se mere på

www.hp.com/go/explorehpsecure

4AA7-3259DAE