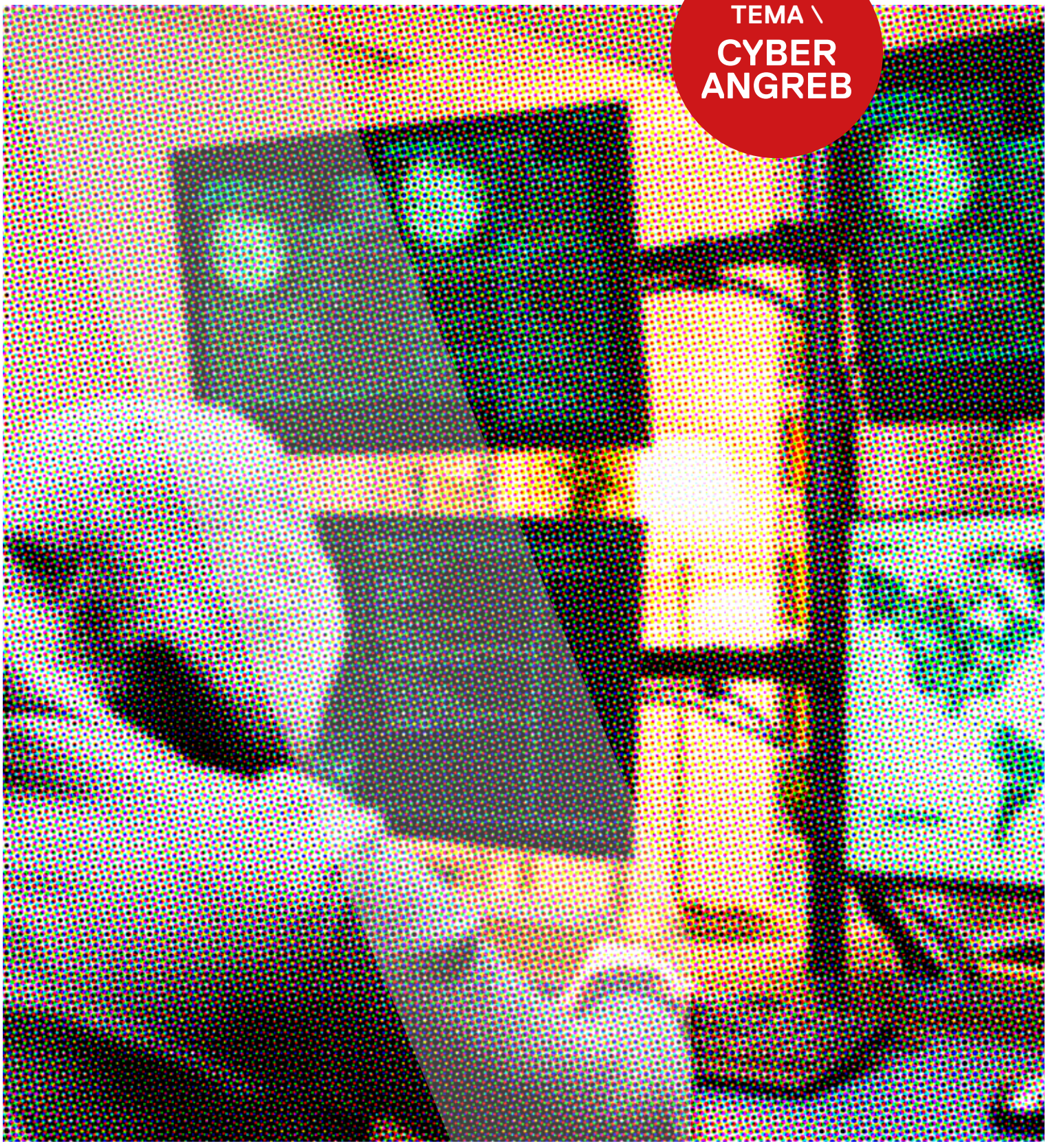
HK BLADET

SAMDATA \ IT-FAGETS FAGFORENING \ HK

MAGASINET

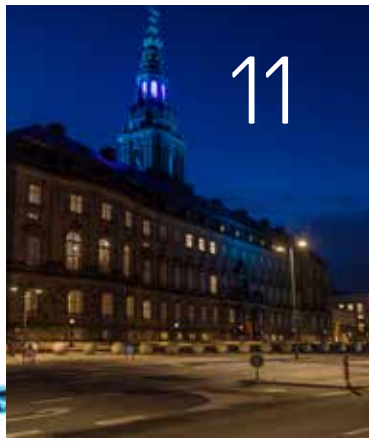
NUMMER 04 \ 2022

TEMA \
CYBER ANGREB



\ INDHOLD

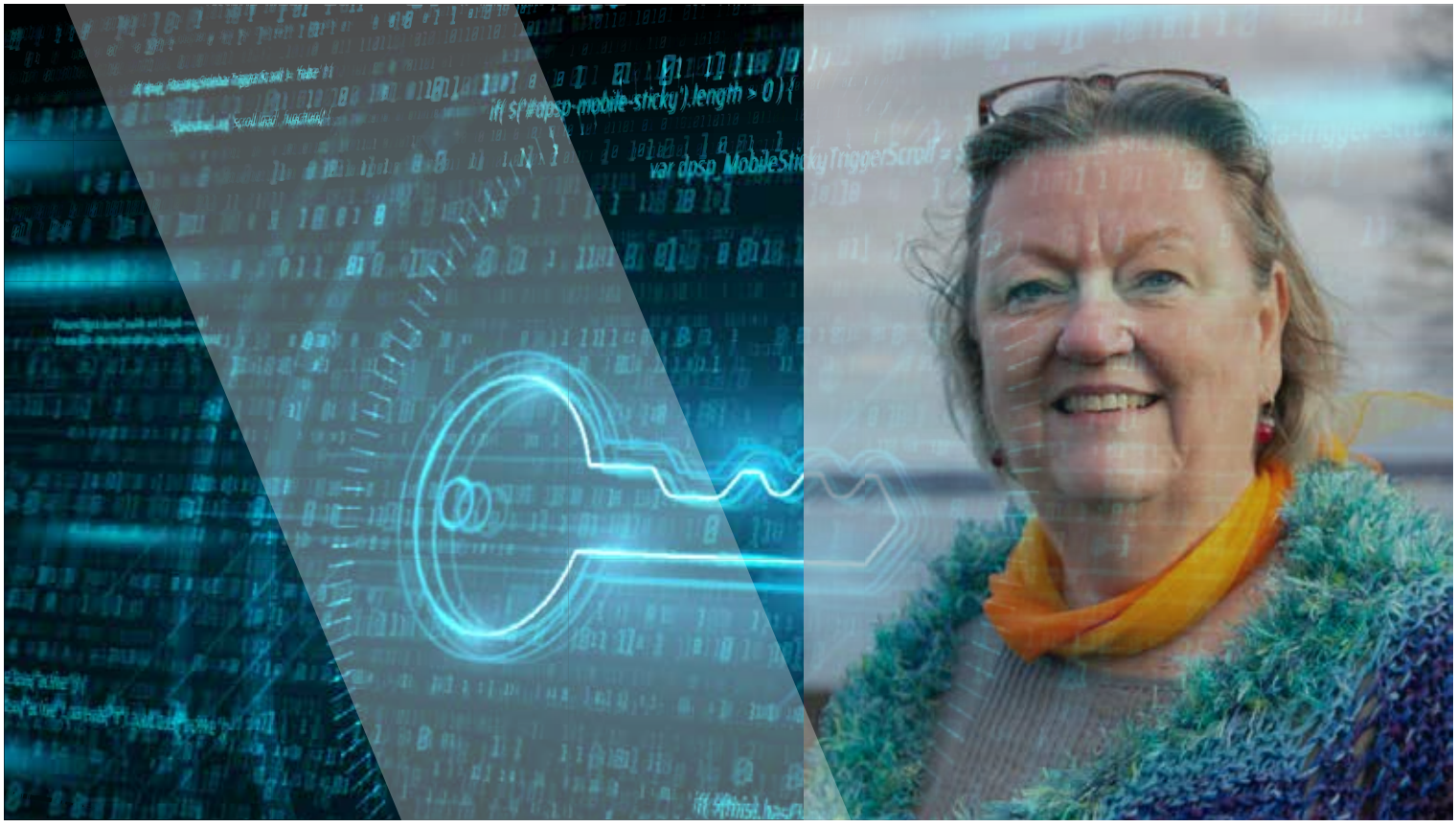
TEMA \
CYBER ANGREB



Udgiver: SAMDATA\HK, Weidekampsgade 8, 2300 København S, samdata@hk.dk, www.samdata.dk \ **Ansvarshavende redaktør:** Per R. N. Nielsen, ansvarlig i.h.t. presseloven
Redaktion: Jeppe Engell, 44je@hk.dk \ ISSN 1604-9349 . TITEL SAMDATA Magasinet . Kopiering og aftryk tilladt med tydelig kildeangivelse. **Grafisk design** www.hillerup-design.com
Grafisk design Henrik Hillerup, www.hillerup-design.com \ **Tryk** JTO A/S \ Oplag 16.000 \ **Næste udgivelse** 24. januar 2023 \

LEDER: CYBERTRUSLEN ER FORDOBLET

Som IT-medarbejder er du virksomhedens bedste forsvar mod IT-angreb. Det er dig, der har viden både om konsekvenserne og forsvarsmulighederne. Derfor er det også dig, der bør sætte emnet på dagsordenen.



Hvis man følger med i medierne, kunne man tro, at de store problemer med phishing, ransomware og DDOS-angreb var et overstået problem.
Medierne beretter kun om Corona, Ukraine, manglen på gas og hyperinflation.
Rækken af katastrofer er lige ved at kunne udløse et angstpræget astma-tilfælde – selv hos ikke-astmatikere.
Det pudsige er, at der er rigtigt langt mellem artiklerne om IT-sikkerhed.
Men dykker man ned i statistikken, så viser det sig, at der næsten er dobbelt så mange firmaer, der bliver angrebet nu – i forhold til for bare to år siden. Det viser statistikker fra SMWDanmark (se grafikken på side 4).
Det er derfor, at vi i SAMDATA\HK – igen – sætter fokus på området med et tema-nummer udelukkende om IT-sikkerhed.

Hold din viden opdateret

Jeg har rodet med computere og IT-sikkerhed hele mit arbejdsliv. Jeg satte mit første backup-system op i 1996 – og det inkluderede både brænding af CD'ere og postvæsenet. I 2006 fik jeg en datamatiker-uddannelse, som har været et fortrinligt grundlag at arbejde videre på.

Men uddannelse skal holdes ved lige. Bare et eksempel: På datamatikeruddannelsen blev vi undervist i Windows Server 2003, og der er sket en hel del siden.
Derfor har jeg været storforbruger af HK's kurser, og har taget hele 39 afsluttede af slagsen, hvis man medregner alt fra en-dages seminarer til de længere forløb.
Det vigtige er: Fem af kurserne har specifikt handlet om IT-sikkerhed, og jeg kan kun anbefale, at du også udnytter de samme muligheder. (Se kursuskataloget side 30-31).

Spark dine kollegaer på kursus

Som IT-eksperter – og måske endda tillidsrepræsentanter – har vi en ekstra forpligtelse til at hjælpe virksomheden med at sætte IT-sikkerhed på dagsordenen.
Stil spørgsmål om de kedelige ting, for det er sjældent ledelsen, der har indsigt i IT-sikkerheden og næppe dem, der har fokus på at tjekke alle hullerne i det digitale forsvar. Uanset jeres forsvar, så er det helt afgørende, at I har et gennemtænkt backup-system, så du kan som udgangspunkt altid spørge, hvor hurtigt I kan få en fuld kopi af alle jeres data.

\ fortsættes side 4

I mange firmaer ser man desværre kurser som en udgift og et tidsrum, hvor medarbejderne ikke "arbejder". Reelt forholder det sig omvendt.
Der er intet, der er bedre for firmaet end, at medarbejderne tager på kursus i IT-sikkerhed. De vender tilbage med ny og opdateret viden, de finder smartere og billigere løsninger.

Bedre cyberforsvar
Heldigvis er der kommet et stort løft i forståelsen for IT-sikkerhed hen over de seneste par år. Skiftende regeringer har investeret massivt i Center for Cybersikkerhed og i forskellige sektorer – f.eks. EnergiCERT – arbejder man fokuseret på at holde kollegaer ajour, så viden om et angreb på én forsyningsvirksomhed kan bruges til at forsvare en anden.
SAMDATA\HK har også været med til at skubbe til udviklingen ved at skabe helt nye uddannelser i netop IT-sikkerhed på Erhvervsakademierne.
Et sundt fokus på data-etik kan også være en god indgang til en debat om IT-sikkerhed.
Det var f.eks. godt at se Datatilsynet stille spørgsmål ved skolernes brug af Chromebooks, uden at skolerne åbenbart kunne svare præcist på, hvor elevernes data blev opbevaret og hvem, der havde adgang til dem.

Det daglige kursus-fix: Følg eksperterne
Som IT-medarbejdere er det en pligt, at holde sig opdateret, og selv om det er godt at gå efter certificeringer og større kurser, så kan det også have stor effekt bare at følge med.
Derfor runder jeg af med et af de små hverdags-hacks, som har gjort det nemmere for mig at følge med.
Jeg bruger LinkedIn ret fast til at følge med rent fagligt og hen over årene har LinkedIn formået at blive en stadig bedre platform for deling af viden. Jeg følger en hel stribe IT-folk, der løbende lufter deres faglige viden, og de gør mig løbende klogere.
Du kan gøre det samme på Twitter, hvor man kan finde lister med hundredvis af IT-eksperter. Hvis man gør det til en fast vane at tilføje fagfolk, når man ser nogen sige noget klogt, så ender man med et være godt klædt på til den daglige kamp mod hackerne.

FAKTA

TRUSLEN MOD DANMARK

Truslen fra cyberspionage: MEGET HØJ
Den vedvarende trussel udgår især fra Rusland og Kina og fører løbende til cyberangreb mod danske mål.

Truslen fra cyberkriminalitet: MEGET HØJ
Den mest alvorlige trussel fra cyberkriminalitet kommer fra ransomware-angreb.

Truslen fra cyberaktivisme: MIDDEL
CFCS hæver trusselsniveauet til middel på baggrund af aktivistiske cyberangreb udført mod europæiske NATO-lande i forbindelse med krigen i Ukraine.

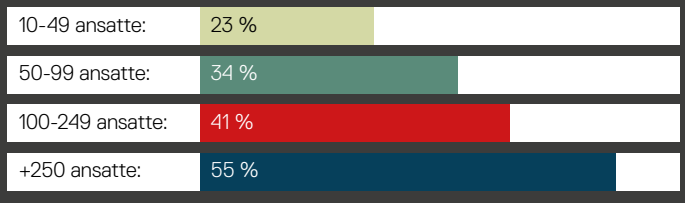
Truslen fra cyberangreb: LAV
Det er mindre sandsynligt at fremmede stater har intentioner om at udføre destruktive cyberangreb mod Danmark.

Truslen fra cyberterror: INGEN
Fraværet af en trussel fra cyberterror skyldes dels at militante ekstremister har begrænset hensigt og midler til at udføre angreb.

(Kilde: Center for Cybersikkerhed – www.cfcs.dk)

KRAFTIG STIGNING I CYBERANGREB MOD FIRMAER

Der er sket en kraftig stigning – stor set en fordobling - i antallet af angreb på danske virksomheder de seneste par år. Det er de største firmaer, der er mest udsat og hver andet firma med mere end 250 ansatte oplever angreb. Men væksten i angreb er størst hos de små firmaer og risikoen for angreb mod firmaer med under 250 ansatte er mere end fordoblet fra 2019 – 2021.



(Kilde: SMVdanmark)

> Jeg har taget fem kurser – udelukkende om IT-sikkerhed – ud fra SAMDATA\HKs kursustilbud. Jeg kan kun anbefale dig at gøre det samme.
>
> Susanne Lyngsaa Henriksen

DEN DIGITALE FRONTLINJE

Døgnet rundt er der indtrængningsforsøg på servere rundt om i Danmark. I Center for Cybersikkerhed forsøger IT-sikkerhedsspecialister at begrænse skaden. Her kan du møde to af dem.

Når hackere forsøger at ramme danske myndigheder og kritisk infrastruktur, er det Center for Cybersikkerhed (CFCS), der er det forreste bolværk. Centret, der hører under Forsvarets Efterretningstjeneste (FE), kan fejre ti-års fødselsdag kort efter udgivelsen af dette magasin. I den periode har de forsøgt at modstå og afhjælpe konsekvenserne af utallige hackerangreb rettet mod både myndigheder og virksomheder landet over.

Bag de blændede vinduer i en anonym kontorbygning på Østerbro i København sidder en række af landets dygtigste specialister indenfor IT-sikkerhed. SAMDA-TA Magasinet har fået lov at komme indenfor for at høre om karrierevejen til at blive digital soldat.

I et af de få mødelokaler, hvor der rent faktisk må medbringes elektroniske enheder, møder vi OB1 og Bonsai. To unge mænd i tyverne, der begge arbejder i Situationscenteret i CFCS, og begge er kommet ind via Cyberakademiet, CFCS' egen uddannelse. Deres rigtige navne er hemmelige, og de optræder i stedet under de navne, som de bruger internt i CFCS.

Hvad går jeres job ud på?

OB1: "Jeg har en operativ koordineringsrolle i Situationscenteret. Det handler om at have ansvar for at få styr på det hele, når en større IT-sikkerhedshændelse rammer. I det interne regi sørger jeg for, at vi griber alle de bolde, der bliver kastet op i luften, og at de bliver spillet i den rigtige retning. Derudover har jeg i det daglige en række administrative opgaver. Jeg startede på Cyberakademiet som analytiker og er sidenhen rykket til denne her rolle (som operativ koordinator og team lead, red.)."

Bonsai: "Jeg er analytiker og vagtholdsleder. Det er den analytiske tilgang til vo-res datagrundlag, hvor vi laver horizon scanning (forudsigelse af angreb, red.) og holder øje med, om der sker angreb. Det handler både om at opdage og imødegå cyberangreb, der er mod Danmark. Rollen som vagtholdsleder er, at man styrer slagets gang. Ikke på et chef-niveau, men man holder styr på de opkald og mails, der kommer ind og koordinerer med de analytikere, man har under sig."

\ fortsættes side 6

Hvad er Situationscentrets opgaver i CFCS?
OB1: "Det er centralnerven for meget af dét, der foregår i huset. Årsagen til det er primært, at vi har meget telefon- og mailkorrespondance med de kunder og interessenter, vi har ude i det danske virksomhedsliv. Det er os, der er kontaktpunktet for langt det meste, hvad angår cybersikkerhedshændelser. Så derfor har vi teten i forhold til, hvad der sker på day-to-day-basis. Vi sørger også for at holde de enkelte interne afdelinger orienteret, om hvad der sker ude i verden. Der er rigtig, rigtig mange henvendelser, der ryger ind til os, og det er os, der triagerer dem og tager et indledningsvist kig på dem. Derefter sender vi det videre der, hvor det nu skal hen. Det kan være en virksomhed, der er blevet ramt af ransomware eller malware, der ringer til os."
Bonsai: "Det hænder også, at vi må ringe ud til virksomhederne, fordi vi hører, at der har været et angreb. På den måde kan det også være os, der tager initiativ til at få et samarbejde op at køre."

Hvordan er I havnet her i CFCS?
Bonsai: "Jeg så det første jobopslag, det var tilbage i 2019, og det synes jeg lød rigtig interessant. Der var jeg lige startet på et IT-studie på et erhvervsakademi, og jeg syntes måske ikke helt, at jeg havde erfaringen til at søge ind. Så gik der et år, og så kom der endnu et jobopslag, og så tænkte jeg, at 'nu har jeg halvt færdiggjort denne uddannelse, nu vælger jeg at søge ind, nu har jeg noget at back'e min ansøgning op med'. Jeg kom ind. Så jeg har en ufærdig uddannelse, men der er rig mulighed for at videreuddanne sig selv herinde, så det anser jeg ikke for et problem."

Hvad var det, der pirrede dig ved opslaget?
Bonsai: "Det første var nok, at der stod FE på jobopslaget, det tænker jeg giver de fleste en interesse. Og så var det bare et velskrevet opslag med IT-muligheder, som jo var dét, mit studie gik ud på, og det jeg interesserer mig for, så det gik hånd i hånd."
OB1: "Jeg har været lidt rundt omkring. Efter gymnasiet gik jeg to år på IT-universitetet, og jeg valgte midtvejs at skifte til en humaniora-uddannelse, som jeg gik på i en rum tid. Det var på dét tidspunkt, at jeg så opslaget, og jeg syntes det var spændende. Jeg søgte derfor og kom igennem den her meget intensive rekrutteringsproces til at blive junior cyberanalytiker."

Hvordan adskiller det sig fra at søge job alle mulige andre steder?
Bonsai: "Det er en meget lang proces med masser af faglige tests og personlighedstests, ligesom der er sikkerhedstjek, som der er for alle FE-ansættelser. Det er en meget lang proces."
OB1: "Mine tidligere erfaringer har primært været med fritids- og studenterjobs. Her er jeg gået op til, hvem end jeg nu har syntes, at jeg ville have job hos, og så sagt: 'Hey, vil I egentlig have interesse for at jeg kom og arbejdede for jer?' Og det har jeg haft succes med. Det her er anderledes. Der er rigtig mange tests, og der foregår en stor fravælgelsesproces undervejs."

Hvad overraskede jer mest ved ansættelsesprocessen?
OB1: "Det blev gjort meget tydeligt, hvor stor vægt der var på det personlige. Det var ikke kun faglige tests, men også psykologsamtaler og samtaler om motivation og vilje. Det er mange personlige parametre, og det skal man navigere i. Man kan mærke, at arbejdsgiveren lægger stor vægt på det, men det er en superfed ting, for det betyder, at det team, der bliver samlet, er velstruktureret. Alle vil det så gerne. Det giver en super god energi i rummet."

Hvad betød jeres uddannelsesmæssige baggrund?
Bonsai: "Det er en meget bred undervisning, man får inden ansættelsen. Det er f.eks. netværk og programmering, og det er ting, som man enten er stærk eller svag på. Jeg følte mig stærkest på netværksdelen, så det var super-godt, at der også blev undervist i programmering."
OB1: "Jeg havde klart mest erfaring med programmering, og dét var også det, jeg

klarede mig bedst i under testforløbet. Men når det så er sagt, så var det også en øjenåbner at komme ind på selve akademiet (Cyberakademiet, red.). Der er jo en årsag til, at vi kommer ind dér, og ikke bare kommer ind i en færdig stilling. Det er, fordi vi også gerne skal formes til at kunne løse forskellige opgaver. Det betyder, at der er rum til, at man kan være svagere i nogle emner og stærkere i andre. Der er jo også mulighed for at lære af hinanden, der er rigtig meget samspil."

Hvordan ser I de langsigtede perspektiver herfra?
Bonsai: "Min situation lige nu er, at jeg skal til at starte på en lederuddannelse. Så jeg tænker, at jeg godt kunne tænke mig at gå den vej. Og det er der også rig mulighed for, ikke kun i Situationscenteret, men også andre steder i FE. "
OB1: "Ja, det er noget, der er blevet spillet med relativt åbne kort med til at starte med. Vores arbejdsgiver er rimeligt klar over, at vi jo er unge mennesker, der ikke har en færdiggjort kandidatuddannelse. Det betyder så, at der skal kunne ligge nogle muligheder i at uddanne sig, imens man arbejder herinde. Jeg er også i gang med en akademiuddannelse i ledelse. Jeg har faktisk allerede skiftet job en gang internt, jeg startede som analytiker og søgte derefter stillingen som operativ koordinator og team lead, som jeg så fik.
Men udover det, så er der også kurser indenfor det faglige. Det kunne være sådan noget som SANS-kurser, præsentationsteknik, håndtering af stressede situationer og andre mindre kurser. Det hele handler om at opbygge en portefølje, så man bliver en robust medarbejder indenfor det her fag."

Hvor er I om fem år rent uddannelsesmæssigt – har du f.eks færdiggjort din kandidat?
OB1: "Nej, det har jeg ikke. Jeg har helt klart fokus på det her med ledelsesuddannelsen. Jeg sidder på nuværende tidspunkt et godt sted for mig, relativt tæt på sektionsledelseslaget, som jeg har en masse støttefunktionsopgaver for. Det vil jeg gerne understøtte yderligere med noget ledelsesuddannelse."
Bonsai: "For mig, så er det mest nærliggende denne her ledelsesuddannelse, som OB1 også er på. Derudover tror jeg, at det faglige for mig kommer til at ligge i certificering, og ikke en reel uddannelse, men det kan jo sagtens nå at ændre sig på fem år."

Hvordan adskiller jobbet sig fra andre jobs i IT-branchen?
OB1: "Vi kører jo 24-7, 365. Der er nattevagter, der bliver varetaget af nattehold. Det betyder, også, at meget af vores job handler om at koordinere på tværs af et 24-timers døgn i stedet for at alle møder 8-16. Der er meget overlevering og asynkront arbejde. Vi skal sikre, at der ikke sker en fragmentering for dem, der sidder i nattevagten. De er stadig en del af organisationen, de møder jo ind på arbejde, bare om natten. De spidsfindigheder skal man have øje for."

Her er der både weekend- og nattearbejde, og man kan formentligt få højere løn i det private erhvervsliv. Hvorfor skal man vælge CFCS i stedet?
Bonsai: "Det er arbejdsopgaverne og det gode kollegaskab. Det sociale spiller en kæmpe rolle, så der er virkelig et ekstremt godt kammeratskab inde i Situationscenteret. For mig er det ikke bare en arbejdsplads. Det er også en vennekreds og en omgangskreds. Samtidig er arbejdsopgaverne superspændende og man får lov til at få indblik i nogle ting, man ellers ikke ville få indblik i."
Ob1: "Man kan meget hurtigt have kig på det dér med løn, men vi har faktisk en rigtig, rigtig fed arbejdsopgave. Det er meget nemt at finde motivationen, for det er Danmarks sikkerhed, vi snakker om. Det er bare rigtig, rigtig nemt at samle sig omkring."

Hvordan kommer det gode kollegaskab til udtryk?
OB1: "Vi har jo vagtrul, og det kan skabe udfordringer, hvis nogen bliver syge. Det sker jo nogle gange. Men det har aldrig været nødvendigt, at chefen har måttet indkalde nogen på vagt. Det sker helt dynamisk uden om ham, at folk træder til. Der er en villighed til, at det skal lykkes. En stor pligtopfyldenhed. Man kan forestille sig andre scenarier, hvor der skal en hård hånd til at sikre, at der bliver dækket ind ved fravær, men her sker det helt automatisk."
Bonsai: "Så sent som i går, der var vi da en håndfuld gutter ude og spille discgolf og drikke en øl eller et glas vand. Det er superfedt. "

Gør det en forskel, at I har været igennem Cyberakademiet sammen?
OB1: "Havde du spurgt mig for fire måneder siden, så havde jeg sagt ja på en meget mere klar måde, end jeg ville gøre nu. Men fordi vi har fået nye medarbejdere ind i vores sektion, som faktisk ikke har været igennem akademiet, og der har vi bare fået dem ind på en rigtigt god måde på rigtigt kort tid. Selvfølgelig betyder tiden på akademiet, at det giver et godt og trygt sted at være, men vi kan faktisk også godt samle de nye op, der ikke er gået den vej."
Bonsai: "Det betyder, at der ikke er nogen spørgsmålstegn ved, om man er god nok. Det er også en kæmpe teambuilding-oplevelse, de der måneder på akademiet. Så det gør virkelig meget for det sociale også, helt uden tvivl."

Vil I give et råd til dem, der er i tvivl om de skal søge?
OB1: "Jeg var meget i tvivl i starten. Så min vigtigste pointe er: Hop ud i det. Prøv at søge. Hvad er det værste, der kan ske? Det er, man får et nej. "
Bonsai: "Jeg vil måske nævne imposter-syndromet, som jeg har hørt at der er flere, der har haft. Når man er kommet ind, så er der flere der tænker på, om de i virkeligheden er gode nok til at være her. Men hvis man er blevet udvalgt, man har været på akademiet og kommer igennem, så er man altså god nok. Det skal der bare ikke være nogen tvivl om – overhovedet. Søg ind, og så væk med imposter-syndromet."

FAKTA

CYBERAKADEMIET

CFCS har oprettet Cyberakademiet, som er en tre måneder lang lønnet uddannelse i en bred vifte af emner indenfor IT, bl.a. "netværksanalyse, programmering, it-sikkerhed og metoder til at håndtere cyberangreb".

SÅDAN HAR VI GJORT

Det er sjældent at statens fremmeste IT-specialister stiller op til interview, og der har da også været en række krav fra FE for at kunne gennemføre dette interview. De to unge mænd er anonymiseret og enkelte detaljer i deres uddannelsesvej er udeladt for at beskytte dem mod identifikation. Det har af samme årsag ikke været muligt at fotografere dem. Samtidig har de fået alle citater til gennemsyn med mulighed for at fjerne ting, der kunne udgøre et sikkerhedsproblem.

\ Af Ernst Poulsen. ernst@ernstpoulsen.com

HVIS DE VIRKELIGT VIL – SLIPPER DE IGENNEM

Der er to helt oplagte typer af angreb, du skal være klar til at forsvare virksomheden mod, fordi de kan lægge jer helt ned: Ransomware og DDOS-angreb. Og så er der lige ti andre typer af angreb, du bør kende.

Egentlig er det en ulige kamp: Kampen mellem hackerne og dem, der skal forsvare firmaets IT-systemer.
"Hackerne vinder før eller siden. Hvis de virkeligt vil ind, så slipper de igennem," siger Brian Harris, der er IT-sikkerhedsekspert hos NCC Group.
"Dem der angriber, har en helt stribe værktøjer på hylden, som de kan bruge, og de behøver egentlig bare at prikke løs fra en ende af, indtil de finder et svagt sted i dit forsvar," forklarer han.
Han har i mere end et årti arbejdet med IT-sikkerhed og hans nuværende job går netop ud på at finde huller i virksomheders IT-sikkerhed: "Pentesting" eller "Offensive Security", som det hedder, når man tester, om man kan trænge igennem i virksomhedernes forsvar.

Hackernes favorit-våben: Dit genbrugs-password
Men før Brian Harris giver et overblik over de vigtigste måder, du bliver angrebet på, så peger han på den største svaghed – på tværs af alle typer af brancher: Genbrug af passwords.
"Vi har alle stribevis af konti på nettet til alt muligt: Facebook, Microsoft, Instagram – og alle mulige sites, hvor vi lige har en brugerkonto. Listen er uendelig, og 99 pct. af os genbruger passwords på tværs af de mange konti," forklarer Brian Harris.
På et tidspunkt vil et af de sites blive hacket, og så ligger tusindvis – hvis ikke millionvis af passwords pludseligt i hænderne på hackere. Hvis de ikke benytter dem selv, kan de tjene penge på at sælge listerne videre på den mørke del af nettet.
"Man kan hente flere terabytes med kombinationer af e-mailadresser og passwords og hackere, der vil angribe bestemte firmaer, behøver blot downloade filerne og så lede efter domænenavne på firmaer, de gerne vil angribe."
"De går i øvrigt sjældent efter specifikke personer, men udnytter blot folk, hvis oplysninger de har fundet fra tidligere lækager."

Ransomware – Hvor er min backup
Et af de våben som hackerne i stor stil har taget til sig de seneste år er Ransomware, hvor hackerne krypterer computere, hvis det lykkes dem at slippe ind.
"Det er helt afgørende, at virksomheder har en 'ransomwareplan', for hvis du først bliver ramt, så er løsningen normalt at slette alt, og geninstallere fra bunden," siger Brian Harris.
Her er det selvfølgelig altafgørende, at man har et backup-system, men også at den plan er gennemtestet, så man ved det virker. Det inkluderer bl.a., at man har et backup-system, der ligger off-site.

OWASP TOP-10

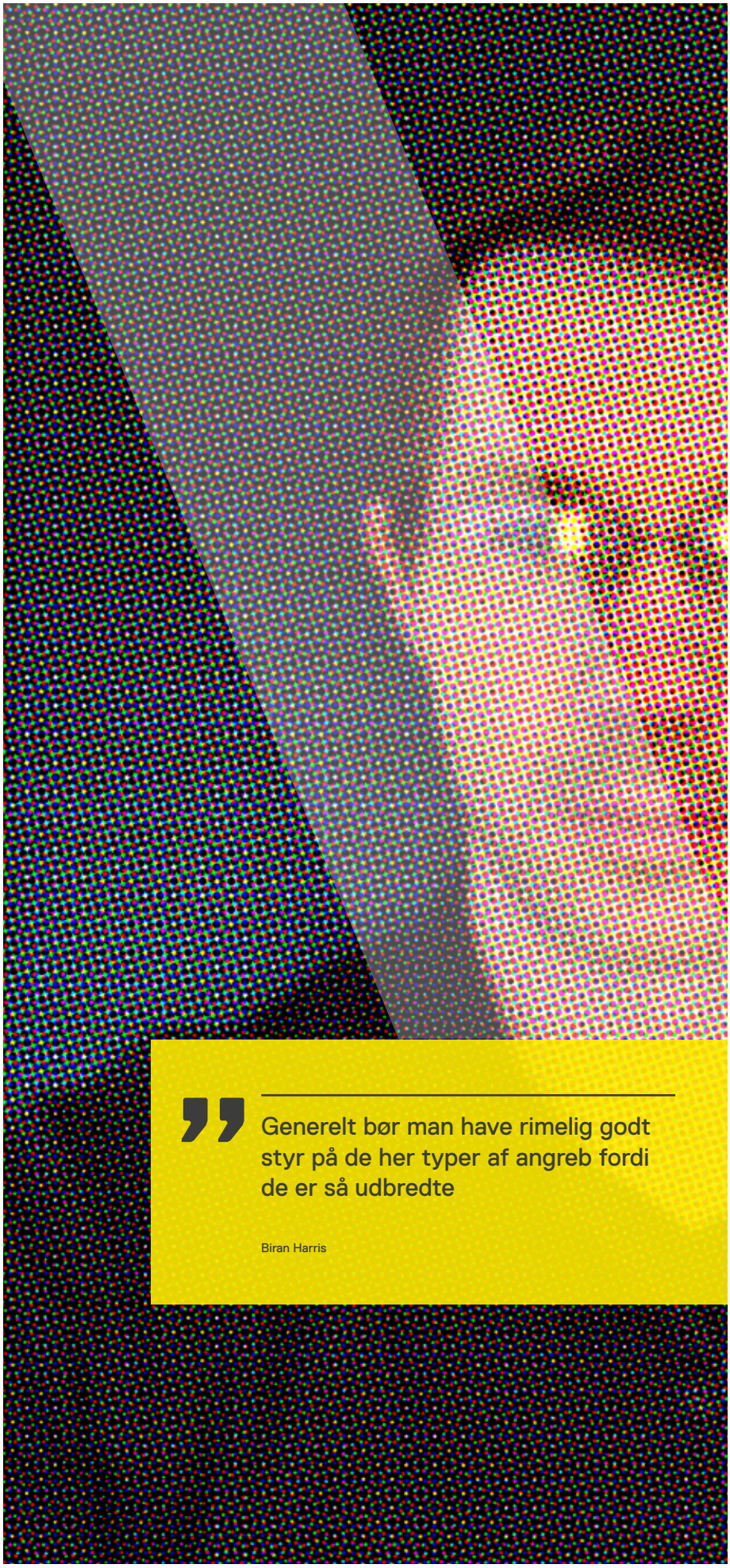
På OWAS.org finder du en oversigt over de ti mest udbredte typer af hacker-angreb.
https://owasp.org/www-project-top-ten/

"Du drømmer ikke om, hvor ofte jeg har spurgt ind til firmaers backups som så viser sig at ligge på servere på samme netværk inde i huset, og så er man lige vidt."
De mere avancerede ransomware-angreb går ikke i gang med det samme, men ligger i dvale et stykke tid, mens de breder sig til de mest basale dele af et IT-system og ikke mindst til backup-systemerne.
Brian Harris ved godt, at han lyder som en, der sælger IT-sikkerhed, men ser ingen vej uden om:
"Det er ikke nok at have en backup. Det er også afgørende, at man får systemet testet, og at det bliver gjort af folk, der har indsigt i alle de ting, der kan gå galt, hvis man bliver angrebet."

DDOS – Har du råd til at blive lagt ned?
Det næste våben i hacker-arsenalet er et klassisk DDOS-angreb, som går ud på at overdænge servere med forespørgsler, så de til sidst ikke er i stand til at svare og går ned. Den type angreb kan stort set bestilles med et par klik på den mere skumle del af nettet.
Angrebet kan enten være fordelt over mange angribende maskiner, som – måske uvidende – lægger maskinkraft til et angreb. En anden variant går mere målrettet efter at lægge forespørgsler på en server, som kræver en masse regnekraft.
"Hvis jeg bruger søgefunktionen til at søge efter noget meget specifikt, skal den blot levere nogle få resultater. Men hvis man beder den om at levere alle tekster med et "b", skal sitet levere langt flere resultater."
Det lyder uskyldigt, for hvad sker der egentlig, hvis jeres firma-hjemmeside er nede i et par timer?
Men for en webbutik kan det betyde millioner i tabt omsætning, eller det kan betyde store administrative udgifter til at rydde op, hvis brugerne ikke kan benytte selvbetjeningsløsninger og begynder at skrive eller ringe til firmaet.
Brian Harris understreger, at løsningen ikke bare er altid at have luft til at modstå angrebet med en hel masse ekstra servere. Det vil være spild af ressourcer og nærmest umuligt.
I stedet bør man rådføre sig med eksperter, der kan hjælpe med de rette værktøjer. Load-balancing, hvor trafikken fordeles ligeligt på servere, kan tage toppen af presset, men er der tale om et større angreb, skal man forsøge at sortere i trafikken.
"Det kan være nødvendigt at blokere for nogle IP-numre, men typisk er man nødt til at lade dem komme ind igen drypvist, for ikke at afvise legitime brugere," forklarer Brian Harris.

Forsvar dig selv: De ti mest aktive angreb
Det varierer hele tiden hvilke typer af angreb, som er mest udbredt blandt hackere, og Brian Harris anbefaler, at man holder øje med udvikling på Wasp.org, hvor Top 10-listen, giver overblik over, de mest aktive typer af angreb.
Øverst på listen står "Broken Access Control", hvor et IT-system giver adgang til mere, end den enkelte bruger egentlig har rettigheder til. Det er et klassisk problem, som har været kendt i tyve år, men som stadig bliver udnyttet på forskellige systemer.

\



> Generelt bør man have rimelig godt styr på de her typer af angreb fordi de er så udbredte
>
> Biran Harris

FYSISK ANGREB:

"DET ER MEGET VÆRRE, HVIS JEG FØRST KOMMER INDEN FOR DØREN"

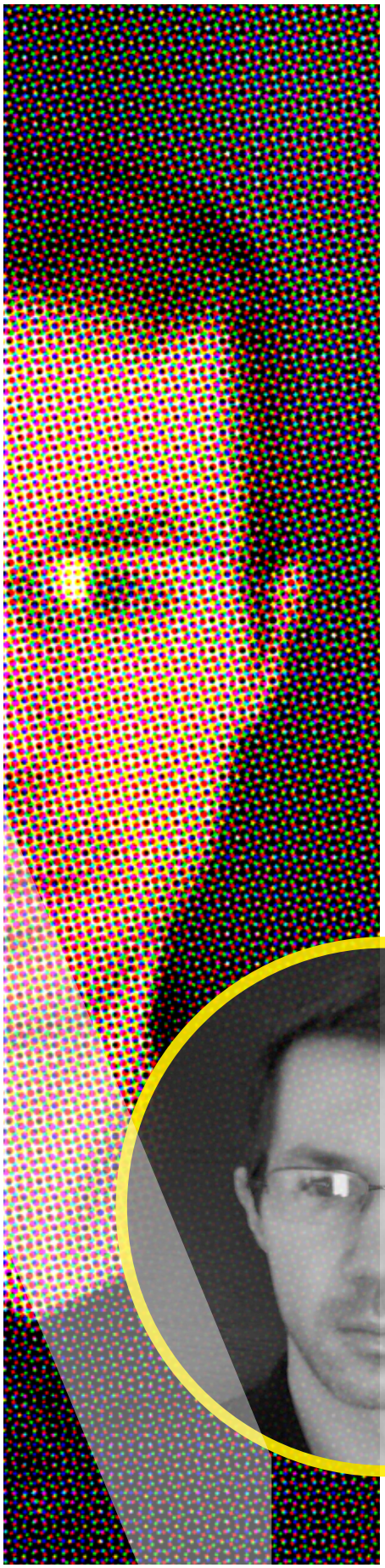
Hvis en hacker ønsker at målrette sit angreb, er noget af det mest virkningsfulde at skaffe sig adgang til et firma rent fysisk. Det er ofte langt nemmere end man tror, fortæller en ekspert.

"Danskerne er meget tillidsfulde, og i Europa tager man ikke fysisk sikkerhed nær så alvorligt, som i andre lande. Det gør det meget nemt, at være hacker," konstaterer Brian Harris.
Han arbejder med IT-sikkerhed hos NCC Group og har gennem årene været udsendt til mindst 10 lande – og her er danskerne altså lidt for nemme. "Russere derimod er meget mere mistænksomme," konstaterer han tørt.

Front-heavy security
Det er meget udbredt, at firmaer har stort fokus på at sikre hovedindgangen, hvor man skal vise adgangskort, hvor der er personale og hvor der er sikkerhedskameraer, der dækker alle vinkler.
"Det er det vi kalder 'Front-heavy-security'', forklarer Brian Harris. Men værdien er sjældent nær så stor, som man tror.
"Jeg er flere gange gået lige ind ad bagdøren, fordi al fokus er på hovedindgangen."
Derefter er der stort set frit spil.
"Når man først er inde, bliver man næsten aldrig spurgt om noget, uanset hvilken etage man færdes på og selv om man ikke har noget adgangs-badge."
"Jeg kan altid finde en bærbar, der står åben og med en USB kan jeg hurtigt installere en key-logger. Så behøver jeg ikke gøre mere, for fra da af, vil jeg få en kopi – i klar-tekst – af alle de brugernavne og passwords vedkommende bruger til at logge på hele systemet."

\ fortsættes side 10

\ Af Ernst Poulsen. ernst@ernstpoulsen.com



Hovedet på skrå

Brian Harris har også trænet sig selv i at spotte de medarbejdere, som er venlige og hjælpsomme. "Det er små psykologiske ting, der røber, om folk er venligt indstillede. Hvis de har hovedet lidt på skrå, lukker øjnene og smiler, så er der store chancer for, at de også vil hjælpe mig, hvis jeg spørger dem om hjælp til f.eks. at komme ind ad bagdøren, hvis jeg fortæller dem, at jeg har glemt mit badge."

Sikkerhedskameraer er angrebspunkt

Brian Harris lever af at teste om virksomheders IT-forsvar er godt nok, og når man har haft den vinkel i mange år, så ser han også ting anderledes.

Sikkerhedskameraer er for ham ikke nødvendigvis noget, der holder kriminelle væk. Tværtimod giver det ofte falsk sikkerhed.

"Der er ingen, der sidder og kigger på kameraer. De bliver kun brugt, når man opdager, at der har været indbrud, men i mellemtiden er de fleste optagelser som regel slettet, fordi det er alt for dyrt at opbevare dagevis af optagelser fra en stribe 4K-kamereaer."

Men kameraer kan også være en svaghed – et decideret angrebspunkt.

"Jeg har haft en kunde, hvor vi testede sikkerheden ved at koble kamera kortvarigt af nettet. Netværket forsøger selvfølgelig straks at forbinde til kameraet igen. Men hvis sikkerheden ikke er i orden, kan den forbindelse nemt indeholde oplysninger, som giver mig adgang til netværket - på admin-niveau," forklarer Brian Harris. "Kameraet burde overvåge mig, men gav mig reelt adgang til alt."

Gamle låsecylindre

Brian Harris tager jævnligt ud og tjekker den fysiske sikkerhed, og her undres han ofte over kvaliteten af helt almindelige låse.

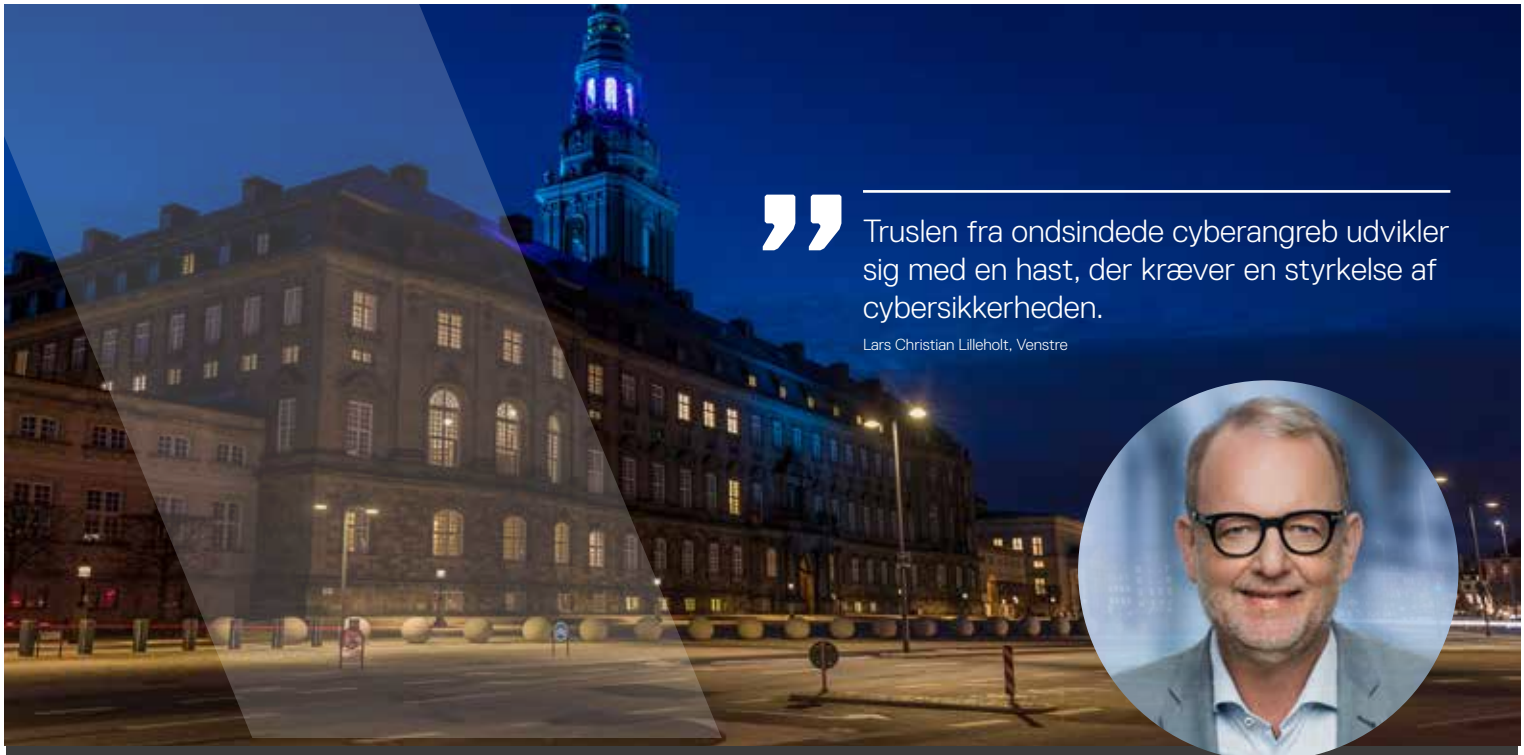
Man skal ikke lede meget på nettet for at konstatere, at hvis cylinderen i en ældre lås stikker blot 2 millimeter ud, så kan den vrides åben på få sekunder. Og selv om låsen er brudt op, er det ikke sikkert, at hackeren vil slå til med det samme.

"Det er mere effektivt for hackeren at skifte låsecylinderen ud med en anden. Dem der arbejder der, vil opleve at låsen fungerer, men hackeren har sin egen nøgle, der gør, at han kan komme og gå, som det passer ham – uden at nogen kan se, hvornår et angreb reelt har fundet sted. Det giver hackeren langt bedre arbejdsvilkår," forklarer Brian Harris.

BLÅ BOG

> Jeg har plantet aflytningsenheder, kopieret laptops og installeret 'bugs' på både printere og dockingstationer. Når jeg først er inden for døren, kan alt lade sig gøre.
>
> Brian Harris, NCC Group

Brian Harris
2020 -
Team Lead for Offensive Security, NCC Group
2020 – 2020
IT Security Architect, Alten Denmark
2018 – 2020
Penetration Tester, L3 technologies
2016 – 2018
Cyber Security researcher, University of Bonn



> Truslen fra ondsindede cyberangreb udvikler sig med en hast, der kræver en styrkelse af cybersikkerheden.
>
> Lars Christian Lilleholt, Venstre

BRED POLITISK FRONT MOD CYBERANGREB

De normale Christiansborg-skærmydsler er lagt på hylden, når det handler om beskyttelse af den digitale infrastruktur.

Smalle aftaler, skænderier, blokpolitik og uenigheder. Konfliktniveauet kan være højt i dansk politik.

Men ser man på de aftaler, der er indgået om at strafforfølge IT-kriminelle og stoppe cyberspionage, så er konfliktniveauet betydeligt lavere. Langt de fleste lovændringer og aftaler på området bliver nemlig vedtaget af brede politiske alliancer.

Da der i 2009 blev indgået dét forsvarsforlig, som dannede rammen for oprettelsen af Center for Cybersikkerhed under Forsvarets Efterretningstjeneste, var samtlige partier undtagen Enhedslisten med – og det samme gjorde sig gældende, da der i 2012 blev indgået nyt forlig.

Enhedslistens kritik af Center for Cybersikkerhed handler blandt andet om, at det organisatorisk hører under Forsvarets Efterretningstjeneste:

"De har ret til og mulighed for at dele alle oplysninger, de kommer i nærheden af, med bl.a. udenlandske efterretningstjenester.

Og det betyder jo sådan set, at Center for Cybersikkerhed helt uforvarende kan være medvirkende til, at informationer, som private virksomheder deler med dem i deres forsøg på at blive beskyttet, kan blive videregivet til amerikanske efterretningstjenester og andre amerikanske virksomheder," sagde partiets daværende retsordfører Pernille Skipper senere til Berlingske Nyhedsbureau i 2014.

Siden da er det blevet til flere brede aftaler om beskyttelsen af dansk IT-infrastruktur, bl.a. en tillægsaftale til forsvarsforliget i 2019, hvor Venstre, Liberal Alliance, Det Konservative Folkeparti, Socialdemokratiet, Dansk Folkeparti og Radikale Venstre vedtog at tilføre yderligere ressourcer til forsvarsområdet, blandt andet for at forbedre beskyttelsen mod cybertrusler.

Ved den lejlighed sagde Henrik Dam Kristensen, forsvarsordfører for Socialdemokratiet:

"Ved tillægsaftalen bliver forsvarsforliget endnu mere robust. I forsvarsforliget satte vi fokus på cyber, og det var der god grund til. Cybertruslen er ikke blevet mindre – tværtimod. Med tillægsaftalen fortsætter vi med fokus på cyber – det er Socialdemokratiet godt tilfreds med."

Da pengene senere blev udmøntet i en konkret plan, sagde Venstres Lars Christian Lilleholt:

"Truslen fra ondsindede cyberangreb udvikler sig med en hast, der kræver en styrkelse af cybersikkerheden. Derfor er det vigtigt, at vi nu sætter ind for at være på forkant med udviklingen. Danmark skal bevare sin position som et af de mest digitaliserede lande, men vi skal samtidig også sørge for at beskytte os bedre mod cyberangreb og nedbrud. Derfor glæder vi os over aftalen, der netop indeholder en række initiativer, der skal sikre dette." \

\ Af Peder Bjerge. peder@bjerge.net .

HK INTENSIVERER INDSATSEN FOR AT FORBEDRE IT-SIKKERHEDEN

Forsvaret mod cyberangreb fra kriminelle og fjendtlige lande kræver specialister. Men manglen på specialister i IT-sikkerhed er så akut og omfattende, at det traditionelle uddannelsessystem ikke vil kunne afhjælpe den, vurderer Jeppe Engell fra SAMDATA. Vi er nødt til at satse på at efteruddanne de nødvendige IT-professionelle. Generelt bør man aktivere langt flere medlemmer i arbejdet for at forbedre IT-sikkerheden. Her er HK med til at gøre en forskel med sine medlemstilbud.

Ikke alene mangler Danmark mange tusinde af IT-specialister. Det kan de fleste arbejdsgivere tale med om.
Men manglen på specialister i IT-sikkerhed er endnu mere akut. Truslen mod de danske IT-systemer er generelt høj, lyder det fra flere sider. Og den ser bestemt ikke ud til at blive bedre. Den russiske cyberkrig mod Ukraine og resten af Vesten har måske øget faren her og nu, men den har også øget den politiske bevidsthed om, at der skal gøres noget.
Men hvor skal vi finde de nødvendige folk til at sikre de IT-systemer, der er afgørende for, at et moderne samfund som det danske kan fungere?
Forudsætningen for at komme frem til et godt svar på det spørgsmål er, at vi i Danmark er nødt til at komme frem til en vigtig erkendelse: Vi kan simpelthen ikke forvente, at det traditionelle uddannelsessystem kan producere nok folk med de nødvendige kompetencer.
"Jeg kan simpelthen ikke se, at det på nogen mulig måde kan lade det sig gøre," understreger Jeppe Engell, IT-faglig sekretær og daglig leder af SAMDATA\HK's sekretariat.

Foto: Amanda Thomsen

Han tilføjer:
"Der er så få IT-sikkerhedsuddannelser og så få, der går på dem, at der er nul chance for, at de kan dække det reelle behov. Hverken DTU, ITU eller erhvervsakademierne kan levere nok specialister i IT-sikkerhed. I stedet er vi nødt til i langt højere grad at anvende efteruddannelse af vores medlemmer til at mobilisere de fagkræfter, som er så vigtige i kampen for at sikre de IT-systemer, der driver vores kritiske infrastruktur. "

Alle skal vide mere om IT-sikkerhed

Men det er ikke nok i sig selv: Vi er nødt til at bevæge os væk fra den vanetænkning, at vi kun skal uddanne folk til at være specialister i IT-sikkerhed, understreger Jeppe Engell.
Den lader vi lige stå et øjeblik.
Jeppe Engells pointe er, at det ikke er nok til at satse på at have eksperter. Alle er simpelthen nødt til at vide mere om IT-sikkerhed, hvis vi skal gøre os håb om at kunne opbygge et tilstrækkeligt værn mod de stadige angreb fra kriminelle og fjendtlige stater som Rusland.
"Langt, langt de fleste ting, vi hører i medierne, hvor virksomheder og andre er blevet ramt af angreb, kunne være undgået, hvis der var anvendt helt banale tiltag som at indføre to-faktor-godkendelse. Det er heller ikke det endelige svar, men det er et skridt i den rigtige retning," siger han.
Alt for mange succesfulde angreb på kritiske IT-systemer handler om, at der er begået tilsyneladende små fejl. Bestemt ikke af ond vilje. Men enhver kan komme til at klikke på et forkert link eller svare på en tilsyneladende uskyldig mail.
Netop derfor vil det være med til at gøre en stor forskel, hvis vi i Danmark generelt kan øge den almindelige opmærksomhed på alle de mange steder, hvor det kan gå galt, understreger Jeppe Engell. Mange små tiltag kan tilsammen gøre en meget stor forskel i det daglige.
Og det behøver ikke være kompliceret.

> Det er fuldstændigt indlysende, at IT-sikkerhed er tæt forbundet med den almindelige sikkerhed på arbejdspladsen.
> Jeppe Engell

De fleste kender til, at de både skal taste deres password ind og derefter godkende med et klik eller en kode på deres mobiltelefon. Den lille ekstra ting kan gøre det ekstra svært og bøvlet for ondsindede hackere eller andre at møve sig ind i de systemer, hvor de ikke har noget at gøre.
"Her er der ikke brug for specialister. Det er noget, vi hver især selv er nødt til at tage ansvar for i hverdagen på jobbet eller hjemmearbejdspladsen. Jeg ved godt, at vi alle sammen bander over, at et kodeord skal være så og så langt, indeholde små og store bogstaver, tal og tegn. Men det er kun, fordi vi ikke lige tænker over de konsekvenser, vi risikerer, hvis vi selv eller vores arbejdsplads bliver ramt," siger Jeppe Engell.

25.000 måtte skifte password

Alt for ofte holder virksomheder det for sig selv, hvis de bliver ramt af et angreb. Men de fleste af os kan mærke det, hvis alle 7-11-butikker i landet må holde lukket, fordi de ikke kan tage imod betaling fra kunderne.
"Eller at DTU for et par uger siden måtte bede 25.000 ansatte og studerende om at skifte password. Så uanset om du arbejder i en stor eller en lille virksomhed, kan konsekvenserne af en fejl, du kommer til at begå, blive meget store og dyre. Og her kunne en lille ekstra sikkerhed som f.eks. to-faktor-godkendelse have forhindret det," siger Jeppe Engell.

"Det er det, vi skal have gjort noget ved," understreger han.
Men det, fortsætter Jeppe Engell, kræver, at HK tager cybersikkerhed ind som et naturligt element, når der bliver udbudt kurser, efteruddannelser eller blot, når den som landets største fagforening repræsenterer medlemmernes interesser.
"Vi skal stille spørgsmål og kræve det, fordi uanset om der er tale om et mindre firma eller en stor koncern, er der HK'ere ansat i mange forskellige funktioner, som regel i supportfunktioner, bogholderi eller marketing. De er altid på arbejde i nøglefunktioner. Så kan vi mobilisere dem til at se sikkerhed som en nødvendighed, kan det være med til at højne sikkerhedsniveauet på arbejdspladserne. Alene det vil skabe meget stærke værn mod cyberangreb i hele Danmark," siger han.

IT-sikkerhed er ikke forbeholdt IT-folk

Lige nu arbejder HK på at finde ud af, hvordan man griber det bedst muligt an. I stedet for at gribe det an på samme måde som andre faglige organisationer som f.eks. Prosa eller IDA, skal HK finde sin egen vej.
"Det involverer ikke kun SAMDATA men hele HK, på alle niveauer, hvor vi skal tænke IT-sikkerhed ind."

\ fortsættes side 14

Et godt eksempel på, hvor HK kan sætte ind i den sammenhæng, er arbejdsmiljøet, fremhæver Jeppe Engell. Han peger på, at HK har arbejdsmiljørepræsentanter overalt på det danske arbejdsmarked, lige fra mellemstore virksomheder til store offentlige arbejdspladser. Hvis de kan komme i spil, vil det gøre en enorm forskel.

"Det er fuldstændigt indlysende, at IT-sikkerhed er tæt forbundet med den almindelige sikkerhed på arbejdspladsen. Det er en del af det, at vores medlemmer skal kunne føle sig trygge på arbejdet, at der er styr på IT-sikkerheden. Så vi skal også sørge for at uddanne vores arbejdsmiljørepræsentanter til at have det med på notesblokken, når de varetager den del af deres ansvar," siger Jeppe Engell.

"Det ligger også lige for at få medlemmer, som måske ikke er så bevidste om, at de arbejder med cybersikkerhed, til at gå ind som ambassadører for IT-sikkerhed. Vi arbejder bl.a. med ideer om at lave nogle kurser eller andre forløb, hvor medlemmer kan få et fagligt input, så de kan tage den rolle på sig."

Dette kunne f.eks. være HK-medlemmer, der i det daglige sidder med arbejdsopgaver, hvor det ville være oplagt at inddrage IT-sikkerhed, påpeger Jeppe Engell.

Satser mere på efteruddannelse

Mens der i dag er mange muligheder for SAMDATA-medlemmer at efteruddanne sig inden for IT-sikkerhed, er der ikke de samme muligheder for andre af HK's mange faggrupper. Så skal man mobilisere dem, er det nødvendigt at tilbyde dem nemme muligheder for at skaffe sig viden indenfor dette felt.

"Det er noget, som vi skal skynde os at gøre noget ved. HK har en unik mulighed for at gøre en forskel, som ikke bare er en chance; jeg vil sige, at det er vores pligt, fordi vi er så stor en organisation med netop den type medlemmer, som sidder i nøglefunktioner spredt ud over det danske arbejdsmarked."

"Vi har kort sagt musklerne til at kunne gennemføre det."

Foto: Amanda Thomsen

> Uanset om du arbejder i en stor eller en lille virksomhed, kan konsekvenserne af en fejl, du kommer til at begå, blive meget store og dyre.
>
> Jeppe Engell fremhæver bl.a., at et såkaldt ransome-ware angreb i gennemsnit koster en mindre eller mellemstor virksomhed 375.000 kr. i tabt omsætning alene. Dette fremgår af en rapport udarbejdet af organisationen SMVdanmark.

HK SÆTTER IND FOR AT FORBEDRE DANSK IT-SIKKERHED

HK vil sætte ind for at øge værnet mod cyberangreb. Ifølge Jeppe Engell, IT-faglig sekretær og daglig leder af SAMDATA\HK's sekretariat, arbejder man i HK på bl.a. følgende tiltag for at forbedre IT-sikkerheden på danske arbejdspladser:

- Bedre efteruddannelse i IT-sikkerhed
- Specialister i IT-sikkerhed er ikke nok: Alle medarbejdere skal vide, hvordan de bedst sikrer deres arbejdsplads mod cyberangreb.
- HK's arbejdsmiljørepræsentanter skal have IT-sikkerhed på agendaen i deres hverv.
- Skabe ambassadører for IT-sikkerhed.
- Netværk for IT-sikkerhed til udveksling af erfaringer og viden.

DI: ALLE VIRKSOMHEDER KAN VÆRE MÅL FOR CYBERANGREB

Foto: Søren Nielsen

Foto: Hans Søndergaard

Krigen i Ukraine ser foreløbigt ikke ud til at have forstærket truslen om cyberangreb mod danske virksomheder. Men hverken store eller små virksomheder kan tillade sig at slappe af. I dag er angrebene fra IT-kriminelle og statshackere så automatiserede, at de kan ramme meget bredt, vurderer Morten Rosted Vang fra DI.

Da krigen i Ukraine brød ud, og Danmark sammen med andre vestlige lande erklærede deres støtte til Ukraine i kampen mod Rusland, lurede usikkerheden: Hvad kunne de russiske IT-kriminelle eller statslige hackere finde på? Hvor godt forberedte var den brede skare af danske virksomheder mod de angreb, der kom fra de stadigt mere automatiserede systemer, der bliver anvendt i den virtuelle krig?

"Blandt virksomheder var der en del usikkerhed i forhold til, hvilke trusler man ville blive mødt med, når Danmark som NATO-land tog aktivt stilling til krigen," siger Morten Rosted Vang, fagleder, digital ansvarlighed og cybersikkerhed i Dansk Industri (DI).

"Situationen kunne jo udvikle sig i den forkerte retning"

Han fortæller, at DI hurtigt efter Ruslands angreb på Ukraine derfor fik lanceret et website med informationer om IT-sikkerhed. Også selv om truslen for almindelige danske virksomheder, i hvert fald ifølge Center for Cybersikkerhed, ikke var større end ellers.

"Men vi opfordrede alle virksomheder, som ikke havde fået opprioriteret cybersikkerhed, til at gå i gang med det som hurtigt så muligt. Situationen kunne jo udvikle sig i den forkerte retning," siger Morten Rosted Vang.

Han understreger, at situationen for den enkelte virksomhed kunne være meget anderledes end gennemsnittet, hvis de f.eks. havde datterselskaber eller partnere i Ukraine.

"Gennem de måneder krigen har varet, har vi ikke kunnet iagttage en øget trussel mod danske virksomheder generelt, men vi kan godt høre på de virksomheder, der er til stede i konfliktområder, at de oplever flere angreb. Mange har også været nødt til at ændre på den måde, de håndterer de trusler," siger Morten Rosted Vang.

> Gennem de måneder krigen har varet, har vi ikke kunnet iagttage en øget trussel mod danske virksomheder generelt, men vi kan godt høre på de virksomheder, der er til stede i konfliktområder, at de oplever flere angreb.
>
> Morten Rosted Vang.

Software-robotter fyrer angreb af

Ifølge ham er virksomheder i Ruslands nærområde som f.eks. Finland og Estland mere udsatte for angreb fra russisk side.

"Her er det et mere akut trusselscenarie end det, vi ser i Danmark, der også påvirker cybertruslen. Men vi er også fuldkommen klar over, at vi ikke kan nøjes med at fokusere på en type virksomhed, når det gælder om at styrke cybersikkerheden, siger Morten Rosted Vang.

- Det er både de helt små virksomheder og de store globale aktører, der har brug for at tage IT-sikkerheden alvorligt. Man skal være opmærksom på, at hele cybertruslen har udviklet sig til at være utrolig automatiseret. Sådan forstået at der ikke nødvendigvis er nogle, som sidder og planlægger, at nu skal de angribe den og den virksomhed. Det er ofte robotter, som fyrer alt mulige angreb af mod alle de sårbarheder, de nu finder, tilføjer han.

\

\ Af Peder Bjerge. peder@bjerge.net .

PROFESSOR ADVARER MOD LURENDE FARE MOD DEN DANSKE CYBERSIKKERHED

Carsten Schürmann, professor på IT-universitetet, frygter, at fjendtlige hackere allerede har installeret bagdøre ind til de systemer, der skal sikre den kritiske infrastruktur i Danmark. I KMD vurderer man ikke den fare som overhængende. Generelt er de danske IT-systemer løbende under angreb fra både kriminelle og lande som Rusland, lyder vurderingen.

I værste fald kan et cyberangreb slukke for strømmen, lukke for vandet eller måske klippe forbindelsen til internettet. Måske rammer et angreb netbanken, så du ikke kan betale dine regninger. Eller også er det hele betalingssystemet, som går ned, og forbrugerne kan ikke betale for den mad, de har lagt i indkøbskurven.
Carsten Schürmann, professor på IT-Universitetet (ITU), Center for Information Security and Trust, understreger, at konsekvenserne af et omfattende angreb på vitale dele af den danske infrastruktur, vi alle tager for givet i hverdagen, kan være enorme og ramme hver enkelt af os. Og måske er det bare et spørgsmål om tid.
"Jeg er bange for, at fjendtlige aktører allerede har installeret bagdørene indtil de IT-systemer, som styrer den kritiske infrastruktur, men de har ikke aktiveret dem endnu, siger professoren på IT-Universitetet (ITU), Center for Information Security and Trust.
Han understreger, at han ikke har beviser for, at det er en realitet, men opfordrer til, at man får det undersøgt. Det er de mest indlysende angrebsmål, hvis Rusland, Kina eller en anden fremmed magt for alvor vil volde skade på en stat, som man opfatter som en fjende.
"Det gælder om at få sikkerhed for, at infrastrukturen ikke er kompromitteret. Man skal i hvert fald være bevidst om, at muligheden er til stede, siger Carsten Schürmann.
Mens de større arbejdspladser som regel har styr på deres IT-sikkerhed, kan mindre virksomheder eller organisationer have sværere ved at opretholde det fornødne beredskab og få lukket evt. svagheder, som kan udnyttes til at skabe bagdøre, mener professoren.

Hvor længe kan huller leve?

Dog skal man holde sig for øje, at den slags svagheder i de vitale IT-systemer, der kan fungere som bagdøre, kun eksisterer så længe, at de ikke bliver identificeret. Lige så snart det sker, kommer der som regel hurtigt en patch, som lukker for hullet ind i systemet, påpeger professoren.
Og det er netop derfor, at Carsten Hvid Challet, Chief Security Officer i KMD, en af de største leverandører af IT-systemer til den danske offentlige sektor, ikke er tilbøjelig til at dele Carsten Schürmanns bange anelser.
"I gennemsnit går der omkring et halvt år, inden svagheder som disse bliver opdaget. Så hvis der er nogle, som har installeret bagdøre, der bare venter på at blive aktiveret, holder de som regel ikke længe," siger han.
Carsten Hvid Challet gør en kort pause:
"Faktum er, at på seks måneder sker der utroligt meget i forhold til efterretninger om svagheder og forbedring af de forskellige redskaber til at modvirke den type bagdøre. Så skal man installere bagdøre, som skal ligge på lur i mere end seks måneder, skal man have fundet svagheder, der endnu ikke er blevet opdaget. Lige så snart de bliver brugt eller opdaget, bliver den viden delt på kryds og tværs. Selvfølgelig er det ikke umuligt, men vi er ovre i noget, som er ekstremt dyrt at udvikle. Der kan være undtagelser, specielt når vi taler statslige aktører, som har ressourcerne og tiden, men her vil man typisk introducere andre foranstaltninger såsom aktiv threat hunting
"Samtidig kan man sætte spørgsmålstegn ved strategien om at anvende den type ressourcer på noget, som man kun måske kan få brug for. Er det ikke nemmere at vente til, at man har brug for at angribe. Personligt køber jeg ikke helt den argumentation, siger KMD's Chief Security Officer.

Har du glemt at låse din hoveddør?

I en eftersætning tilføjer han, at større virksomheder eller organisationer har typisk så store, og dermed komplekse, systemer, at der nok skal være svagheder at angribe, hvis det måtte blive nødvendigt.
"Hvis de endelig vil ind, er det ikke umuligt. I bund og grund ligner den slags angreb et almindeligt indbrud i IT-systemer. Måske anvender de phishing eller social engineering. Måske andre redskaber. Det er egentligt simpelt: Hvis man har glemt at låse sin hoveddør, går tyvene ind af den, eller et andet sted. De skal såmænd nok finde en eller anden svaghed. Så det at bruge tid og ressourcer på at installere egne bagdøre, der skal ligge længe, virker ikke sandsynligt, siger Carsten Hvid Challet.
Generelt mener han, at man bør skelne mellem de forskellige typer angreb. En form for cyberangreb er blevet anvendt som en form for terror vendt mod Ukra-

ine, hvor russerne bl.a. har forsøgt at blokere eller hæmme modstandernes evne til at kommunikere elektronisk. Når det kommer til de såkaldte bagdøre, handler det derimod først og fremmest om spionage.
"Her gælder det om at være til stede i systemerne uden at blive opdaget. I den forbindelse går de efter forskellige mål, alt efter hvilket formål der er tale om," siger Carsten Hvid Challet.
Han understreger, at man i KMD deler opfattelse omkring trusselsvurderingen med Center for Cybersikkerhed (CFCS). Her vurderer man ikke, at trusselsbilledet har ændret sig synderligt som følge af krigen i Ukraine, hvor Danmark sammen med de fleste NATO-lande vendte sig kraftigt mod det russiske angreb på Ukraine. Umiddelbart kunne det lyde som en tilforladelig tilgang til IT-sikkerhed, indtil Carsten Hvid Challet med henvisning til den seneste trusselsvurdering fra CFCS tilføjer, at truslen mod danske mål er høj.
"Ikke mindst truslen fra Rusland og Kina," siger han.

Stilhed før stormen

Som et kuriosum nævner Carsten Hvid Challet, at normalt kunne man se en lang række angreb fra den side, men lige efter krigen brød ud i februar var der med KMD-mandens ord "utroligt stille."
"Altså som at der skete intet. Nu er vi tilbage i nogenlunde det samme trusselsbillede som før krigen. Jeg ved godt, at der var mange i medierne, som råbte højt om en storm mod Danmark, men det var altså ikke noget, vi kunne observere, siger han.
Carsten Hvid Challet tilføjer:
"Men vi i Danmark er heller ikke hovedmålet for den slags aktivitet, som følger den type krigsførelse. Her er der måske nogle andre områder, som er i fokus. Vi har set mange flere angreb mod f.eks. ukrainske mål. Også i Rusland er man nødt til at prioritere sine ressourcer."
I den forbindelse bør man også i Danmark prioritere indsatsen, mener Carsten Schürmann. Særligt bør man arbejde for at styrke modstandsdygtigheden overfor cyberangreb i de mindre og mellemstore virksomheder. I denne del af erhvervslivet er der sjældent nok penge og tid til at afsætte en eller endda flere medarbejdere til at koncentrere sig om, at IT-sikkerheden er god nok.
"Man skal gøre sig klart, at truslerne mod Danmark og den danske infrastruktur, ikke kun handler om de store virksomheder eller det offentlige, siger Carsten Schürmann. Han henviser til, at angrebene ofte kan ramme mindre virksomheder, som måske er leverandører til større firmaer, der så kan blive ramt indirekte.

> Jeg er bange for, at fjendtlige aktører allerede har installeret bagdørene indtil de IT-systemer, som styrer den kritiske infrastruktur, men de har ikke aktiveret dem endnu.
>
> Carsten Schürmann

Foto: www.itu.dk

> Hvis de endelig vil ind, er det ikke umuligt. I bund og grund ligner det et almindeligt indbrud. Hvis man har glemt at låse sin hoveddør, går tyvene ind af det. Ellers finder de en anden svaghed.
>
> Carsten Hvid Challet

Russiske angreb på infrastruktur indtil nu

Ifølge Carsten Hvid Challet vil russiske angreb på Danmark sandsynligvis først og fremmest koncentrere sig om at indsamle informationer f.eks. i forhold til det danske NATO-medlemskab eller afsendelse af krigshjælp til Ukraine. Samtidig vil det også være oplagt at forsøge at ramme den kritiske offentlige infrastruktur som elforsyning eller vandforsyning. I den forbindelse skal man se begrebet mere bredt; også private virksomheder er en del af den infrastruktur, både almindelige borgere, erhvervslivet og det offentlige er dybt afhængig af. Tag f.eks. internettet eller bankerne.
"Man så det f.eks. i angrebet på Viasat, hvor russerne gik efter at lukke satellitkommunikation ned, siger han.
Dette angreb skete den 24. februar, samtidig med at russerne angreb Ukraine. I maj udsendte den danske udenrigsminister Jeppe Kofoed en pressemeddelelse, hvor man entydigt pegede på Rusland som ansvarlig for angrebet på det amerikanske internet-satellit-firma Viasat.
"Dette angreb viser endnu engang Ruslands totale mangel på respekt for internationale regler og normer. Det viser tydeligt, hvorfor der er brug for at styrke det internationale samarbejde for at bekæmpe cybertruslen," lød det fra den danske minister dengang.
Skal Carsten Hvid Challet give sit bud på, hvor godt Danmark klarer sig i forhold til andre lande, når det gælder om at beskytte sig mod bl.a. russiske cyberangreb, trækker han på smilebåndet:
"Det er lidt svært at vurdere. I bund og grund har vi kritisk infrastruktur og forskellige sektorer, som er beskyttet på forskelligt niveau. Lad os tage vandværkerne f.eks. Jeg tvivler ikke på, at de store vandværker har tilstrækkeligt med penge til at sikre sig godt, men så har du måske et mindre vandværk ude i provinsen, der har færre ressourcer til at hindre cyberangreb. Generelt kan det bedre svare sig at angribe den type mål."
Hans pointe er, at det er vanskeligt at svare entydigt på, hvor godt danskerne er sikret mod cyberangreb. Men tager han en gennemsnitsbetragtning er Danmark godt med, men det er ikke det samme som, at de russiske angreb ikke kan trænge igennem og forøve skade.

\ Af Ernst Poulsen. ernst@ernstpoulsen.com

LANGT FLERE HACKERANGREB MOD FORSYNINGSVIRKSOMHEDER

Selv om hackerne på europæisk niveau er blevet meget bedre til at trænge igennem forsyningsvirksomhedernes forsvar, så er det kun en håndfuld danske virksomheder der hidtil er ramt.

Ved første øjekast ser det ud til, at hackerne på blot få år, har fået langt større succes med at angribe infrastruktur som el-selskaber, vandværker og fjernvarmeværker.

En rapport fra EnergiCERT viser nemlig, at antallet af succesfulde angreb på europæiske energiselskaber er steget fra to om året i 2015 – til hele 20 alene for den første del af 2022.

Men neden under de tal er billedet langt mere kompliceret, fortæller Søren Maigaard, der er direktør i EnergiCERT. I virkeligheden kan der have været et stort mørketal tidligere, vurderer han.

"Man er blevet meget bedre til at dele viden i sektoren. Der er ganske simpelt kommet en langt større forståelse for vigtigheden af at dele viden om IT-angreb, så man kan forhindre, at de samme angrebstyper kan ramme flere firmaer."

Han peger på Mærsk som et af de firmaer, der har skabt en større forståelse for vigtigheden af at dele viden efter at shipping-giganten tabte tæt ved to mia. kr. da de blev ramt af ransomware i 2017.

"Det har også den store fordel, at man som virksomhed er med til at styre narrativet. Hvis man ikke siger noget, risikerer man at andre overtager fortællingen, og så ser det ikke altid så positivt ud."

De går efter pengene

Søren Maigaard lægger også vægt på, at den gennemsnitlige hackers formål ikke er at lægge infrastrukturen i samfundet ned.

"De går hovedsageligt efter at tjene penge på ransomware, og når de angriber bredt, så sker det af og til, at de rammer forsyningsselskaber. Selv om der har været klare angreb på energiforsyningen i Ukraine, så har vi ikke set en øget mængde af angrebsforsøg mod danske virksomheder fra Rusland."

Samlet set fortæller han, at der er ca. 3.000 IT-angreb i timen mod forsyningssektoren, og set i det lys, mener han, at de seks angreb som har været succesfulde mellem 2015 og 2022 (se faktaboksen), er et relativt lavt antal.

Han peger på, at der er kommet en større bevågenhed i branchen – især på vigtigheden af at skelne de almindelige administrative IT-løsninger fra den operationelle teknologi (OT).

Foto: Ernst Poulsen

> Hackerne opgraderer hele tiden og finder på nye og smartere metoder. Så hvis man bare gør det samme som sidste år, så er man allerede bagud.
>
> Søren Maigaard, direktør EnergiCERT

Forude er der dog også risiko-elementer

En af årsagerne til, at hackerne har mere succes i dag, er, at der er sket et teknologi-skifte i forsyningsvirksomheder. Tidligere benyttede man sig af proprietære systemer, men nu er langt flere Windows-baserede, og derfor er der i dag en øget risiko for at blive ramt, når hackerne skyder med spredehagl for at finde systemer, der er sårbare over for ransomware.

Derfor mener Søren Maigaard også, at forsyningsvirksomhederne bliver nødt til at følge med på sikkerhedsområdet.

"Hackerne opgraderer hele tiden og finder på nye og smartere metoder. Så hvis man bare gør det samme som sidste år, så er man allerede bagud. Man er nødt til at opgradere sit forsvar hele tiden," understreger Søren Maigaard.

FAKTA

SÅDAN BLIVER ENERGISEKTOREN ANGREBET

\ 48 angreb mod europæiske energiselskaber fra 2015 – 2022
\ 31 var ransomware-angreb
\ 15 angreb påvirkede OT-netværket
\ 13 angreb inkluderede også data-tyveri
\ 3 angreb med data-tyveri som hovedfokus
\ 2 spionage-angreb

DE BLEV RAMT AF CYBERANGREB 2015-2022

\ Næstved Fjernvarme
\ Isoplus Fjernvarmeisolering
\ Tønder Forsyning
\ Kalundborg Forsyning
\ Vestas
\ LIFA

STIGNING I ANTALLET AF SUCCESFULDE ANGREB

2017:	3
2018:	2
2019:	10
2020:	10
2021:	20

\ fortsættes side 20

Læs mere

\ Cyberangreb mod europæiske energi- og forsyningsselskaber
kortlink.dk/2gpm7

\ Cyber- og informationssikkerhedsstrategi for el-, gas- og fjernvarmesektorerne 2022-2025
kortlink.dk/2gpm6

SÅDAN BLEV VANDVÆRKERNE ANGREBET

Mindst seks gange er det lykkedes for hackere at infiltrere danske forsyningsvirksomheder – bl.a. hos to vandværker, der blev lagt ned af ransomware. Det fik i sidste ende ikke betydning for borgerne, men i nogle timer, mistede man overblikket over driften.

KALUND-BORG

"VI MISTEDE OVERBLIKKET"

En torsdag aften i august 2021 gik SRO-anlægget på Kalundborg Forsyning pludseligt ned. Systemet bruges til at overvåge både vandværk og spildevand og medarbejderne kæmpede forgæves med at få kontrol over anlægget, men måtte kaste håndklædet i ringen.
Det var lykkedes hackere at infiltrere selskabets computere med ransomware, og computerne var derfor låst og kunne ikke benyttes.
"På det tidspunkt anede vi ikke, om vores anlæg kørte. Vi er i blinde, når vores SRO er nede, så vi måtte have folk ud på renseanlæg og vandværker for at finde ud af, om vi stadig var i drift," udtalte direktøren for Kalundborg Forsyning til magasinet "Dansk Vand".
I løbet af 12 timer lykkedes det at få kontrol over anlægget igen og ved hjælp af IT-leverandøren får man genoprettet systemet med hjælp fra en backup, der var taget tidligere på dagen.
I den efterfølgende evaluering konkluderede Kalundborg Forsyning, at det var afgørende, at man havde en beredskabsplan, så man vidste hvem der skulle kontaktes, og hvordan forløbet skulle foregå. Man overvejer stadig om der i højere grad bør være manuelle alternativer til den elektroniske styring.

TØNDER

ALT MÅTTE KØRES MANUELT I TO MÅNEDER

Tønder Forsyning fik låst deres computere i et ransomware-angreb i sommeren 2020. Samtidigt blev 50 Terabyte data slettet på et minut.
De måtte derfor klare sig uden administrative-systemer og SRO-system (Styring, Regulering, Overvågning) i hele to måneder.
Angrebet kom ind via telefonsystemet, men nåede at brede sig til at de øvrige systemer. Senere har man fundet ud af, at der var tale om et såkaldt zero-day angreb, hvor hackerne har benyttet en hidtil ukendt svaghed i systemerne.
Ifølge tech-sitet Version2.dk kostede det samlede angrebet Tønder Forsyning et to-cifret millionbeløb og for borgerne betød det bl.a. at de i flere måneder ikke kunne få overblik over deres vandforbrug.

\ Af Peder Bjerge. peder@bjerge.net .

SÅDAN FORSVARER FINNERNE SIG MOD DE RUSSISKE CYBERANGREB

Efter at have set den russiske nabo opføre sig stadig mere aggressivt, har Finland udviklet et eget totalforsvar mod russiske cyberangreb, hvor store dele af samfundet er mobiliseret som værn mod de digitale angreb på den vitale infrastruktur. I et interview med SAMDATA Magasinet forklarer en af arkitekterne bag det finske cyberforsvar, hvordan finnerne gik til opgaven med at værne alle dele af deres samfunds infrastruktur mod Ruslands angreb.

\ fortsættes side 22

> Vi lever i en virkelighed, der gør, at vi skal være parat til at reagere hurtigt. Det har stået klart for os i årtier.
>
> Aapo Cederberg

Den russiske bjørn bor lige på den anden side af den stiplede linje, der på landkortet adskiller Finland og Rusland. I det 20. århundrede har finnerne kæmpet to krige mod Sovjetunionen, hvor de mistede mere end ni procent af deres areal.
"Vi lever i en virkelighed, der gør, at vi skal være parat til at reagere hurtigt. Det har stået klart for os i årtier, siger Aapo Cederberg, tidligere oberst i det finske forsvar og leder af det hold af analytikere, som udtænkte den særlige finske forsvarsmodel.
Med Ruslands blodige overfald på et selvstændigt Ukraine måtte finnerne indse, at de ikke længere kunne være sikre på, at russerne vil respektere deres selvstændighed. Den finske statsminister Sanna Marin beskrev situationen således den 3. maj i år:
"Ruslands invasion af Ukraine har ændret den sikkerhedspolitiske situation i en sådan grad, at det ikke er muligt at vende tilbage til den måde, tingene var før. Vi kan klart se, hvor Rusland vil have os hen."

Finsk totalforsvar mod cyberangreb

Aapo Cederbergs arbejde for det finske forsvar er dog ikke inspireret af de sidste otte måneders krig i Østeuropa. Det begyndte for mere end 12 år tilbage i tiden, hvor Finland stadig holdt sig uden for de vestlige forsvarsalliancer

Finland gik over til et totalforsvar overfor cyberangreb i 2010; ifølge Cederberg har konceptet sine rødder i den kolde krigs ide om, at i tilfælde af krig kan hele nationen mobiliseres i krigsindsatsen. Noget et lille land som Finland er nødt til, hvis det skal kunne klare et angreb fra den meget større nabo.
Han peger på, at den tilgang passer meget godt til cybersikkerhed, fordi et effektivt forsvar af landets IT-sikkerhed skal ses i bred forstand; herunder også private virksomheder, der driver IT-netværk og medieplatforme, hvor cyberkrig udkæmpes.
I dag er Cederberg ikke længere en del af det finske forsvar. Han er medstifter og partner i den finske virksomhed Cyberwatch Finland, der rådgiver virksomheder, byer og lande om, hvordan de bedst sikrer sig mod cyberangreb.
Interviewet med SAMDATA Magasinet foregår over Google Meet, hvor Aapo Cederberg har taget lidt tid ud af sin ferie i sin svenske ødegård til formålet.
Som det første fremhæver han, at man er nødt til at se det store billede, hvor den russiske stat har forskellige magtmidler at anvende. Lige fra direkte økonomisk pression, som Rusland har anvendt for at få de vestlige lande til at holde sig fra at hjælpe Ukraine med våben eller sanktioner, til direkte at bruge militærmagt, hvor angrebene i 2014 og 2022 på Ukraine blot er et af de seneste eksempler på dette.
"I de senere år har de dog mest anvendt cyberangreb og hybrid krigsførelse for at nå deres mål," siger han.

Kendte russiske metoder

Cederberg fremhæver, at man først er nødt til at forstå den russiske fjende for at kunne opbygge et tilstrækkeligt forsvar.
Den klassiske fejl, vi i Vesten begår, er at se det med vestlige øjne. I stedet er vi nødt til at sætte os ind i den russiske mentalitet for at finde et effektivt forsvar mod deres angreb, lyder hans konklusion. Kort sagt, i stedet for at følge vestlige meningsmaskiner, må man gå direkte til de russiske kilder, lyder hans opfordring.
"Mange russiske militære analytikere har offentliggjort deres arbejde i artikler og forskellige medier. Gerasimov (Valery Vasilyevich Gerasimov, chef for den russiske generalstab, red.) har anvendt disse metoder, som de ikke kun har brugt i Ukraine. Vi har set det i Syrien og før det i Georgien. Det er en udvikling, vi har kunnet følge over årene," siger Aapo Cederborg.
"Rusland er et af de bedst udrustede lande til at gennemføre cyberangreb, ofte i tæt samarbejde med Kina," konkluderer han.
Den russiske kapacitet til at føre cyberkrig er opbygget anderledes, end man f.eks. ser i de vestlige lande, hvor den slags er organiseret som en del af statsapparatet, i efterretningstjenesten eller som en del af militæret. I Rusland har efterretningstjenesterne FSB og SVR, der begge udspringer af Sovjetunionens KGB, hver deres netværk af forbryderorganisationer at trække på til at foretage cyberangreb. Den kombination har vist sig at være et meget effektivt våben, man bør have respekt for, lyder Cederbergs pointe.
"I det omfattende cyberangreb på Estland i 2007 var det ikke den russiske stat, som stod bag, i hvert fald officielt, men kriminelle organisationer eller bander. Ofte kan det være kompliceret at få et klart billede af, hvad Rusland egentlig kan, fordi meget bliver outsourcet til de kriminelle, der ved siden af også angriber IT-systemer for økonomisk gevinst. Men hvis du ser på, hvor mange angreb de har gennemført i USA og nu i Europa, får du et godt billede af, hvad russerne er i stand til i dag," siger Aapo Cederberg.

Erkender den stigende fare for cyberangreb

Tilbage til arbejdet med at finde et effektivt forsvar mod den trussel: Den stadigt stigende russiske aktivitet i dette grænseland kom i 2010 øverst på den finske agenda.
"Der erkendte vi i Finland, at den type angreb er en brændende trussel for et moderne samfund, der gennem årene er blevet mere og mere afhængig af IT. Hvis et cyberangreb lammer blot noget af vores kritiske infrastruktur, vil vi få alvorlige problemer. Derfor er det så vigtigt at have et forsvar, som spænder over hele vores samfund," siger Aapo Cederberg.
I arbejdet med at udforme et effektivt forsvar var man derfor nødt til at se på, hvordan det finske samfunds infrastruktur er opbygget. Selv om mange

> Cybersikkerhed skal også indgå som en del af uddannelsessystemet. Man er nødt til at uddanne hele samfundet.
>
> Aapo Cederberg.

vestlige lande kan synes ens, er der ikke en one-size-fits-all, man kan bruge her. Selv ikke i Skandinavien. Cederberg fremhæver, at nok er f.eks. Danmark og Finland ens på mange punkter, men der er også markante forskelle: Man er nødt til at tage udgangspunkt i, hvem der konkret driver landets kritiske infrastruktur.

"Alle de dele af samfundet, der udgør eller bidrager til infrastrukturen, vil være oplagte mål for angreb. Så man skal have nøje defineret, hvem der er afgørende for at få infrastrukturen til at fungere, uanset om det er offentligt eller privat. Det er altafgørende at få foretaget den analyse rigtigt og finde ud af, i hvor høj grad de er i stand til at modstå cyberangreb, siger Aapo Cederberg.

Han understreger, at man ikke kan se den kritiske infrastruktur som noget, der kun handler om det offentlige. Alt efter hvordan samfundet i det enkelte land er skruet sammen, vil private virksomheder direkte drive mere eller mindre af infrastrukturen eller optræde som leverandører til det offentlige. Og de er alle mulige mål for cyberangreb.

Militæret er kun ansvarlig i tilfælde af krig

Så alle disse er nødt til, hver især og uafhængigt af hinanden, at kunne modstå cyberangreb. Hele det finske forsvar mod cyberangreb er decentralt opbygget i modsætning til f.eks. USA, UK eller Israel, hvor der er et centralt forsvar mod den type angreb. Særligt i Israel er man meget dygtige til at håndtere cybertrusler, understreger Cederberg. I Finland går staten derimod kun ind og tager en styring, i tilfælde af en direkte væbnet konflikt, fremhæver han.

"Selvfølgelig har militæret et godt beredskab og kapaciteterne til at håndtere cyberangreb. Men i Finland er det kun tilladt for militæret at overtage ansvaret for at beskytte civilsamfundet i tilfælde af krig. I fredstid ligger ansvaret ude i de enkelte virksomheder, myndigheder og organisationer. En central styring som man ser i Israel eller USA ville være alt for dyrt for et land som Finland."

Dette indebærer, at i hvert fald de vigtigste virksomheder og det offentlige skal have et klart beredskab mod cyberangreb, understreger han. Her er det afgørende, at den øverste ledelse på hver enkelt arbejdsplads har cybersikkerhed med i deres overvejelser.

"I tilfælde af et angreb eller en krise, skal de have et klart beredskab til at håndtere en sådan situation. Igen, skal man forstå, at man ikke opnår den bedst mulige cybersikkerhed gennem militæret, efterretningstjenester eller politiet. I stedet skal det gennemsyre hele samfundet."

Det bedst mulige hold på plads

Ifølge Aapo Cederberg er det derfor vigtigt, at man deler viden og erfaringer på tværs af det offentlige og private, så hver enkelt arbejdsplads har det bedst mulige hold på plads til at håndtere en skarp situation.

"Hvis ikke man får opøvet disse færdigheder og beredskab, står man dårligere overfor angreb," siger han.

Men hvis man tror, at cybersikkerhed er noget for de få, altså chefer og specialister, tager man fejl. Udfordringen er, at et moderne samfund er en kompliceret størrelse, en maskine med et utal af bevægelige dele, hvorfor cybersikkerhed er et emne, som alle dele af samfundet er nødt til at være bevidst om.

"Cybersikkerhed skal også indgå som en del af uddannelsessystemet. Man er nødt til at uddanne hele samfundet," pointerer Aapo Cederberg.

Hov stop, skal børn så også have undervisning i cybersikkerhed, kunne et nærliggende spørgsmål lyde. Svaret kommer prompte og uden tøven.

"Ja, selvfølgelig."

Børn og unge er også digitale væsner, der er nødt til at forstå, hvordan de undgår at blive ramt eller brugt i et cyberangreb.

I et moderne samfund er cybersikkerhed en størrelse, man er nødt til at tænke ind i alle de dele af hverdag, der er digitaliseret, uanset om det er på jobbet henne på kontoret eller hjemme i privaten, hvor mange efterhånden har arbejdscomputeren åben for mails og Zoom-møder.

"I dag er vi også ekstra udfordret, fordi vi, bl.a. under pandemien, arbejder mere og mere hjemmefra. Det giver nogle nye udfordringer i forhold til at sikre data. Den udvikling giver russerne mange flere angrebsmuligheder for at ramme vigtige dele i samfundet," fortsætter han.

\ Af Peder Bjerge. peder@bjerge.net .

ESTERNE LEVER I SKYGGEN AF RUSSISKE CYBERANGREB

Det lille baltiske land var i 2007 udsat for så hårde russiske cyberangreb, at myndighederne i dag har det nødvendige beredskab til at modstå nye anslag. Ifølge en britisk forsker i landet har mange vænnet sig til, at de russiske angreb gør det lidt sværere at agere digitalt. Men faren for et digitalt altødelæggende Pearl Harbor-angreb i år synes at være drevet over.

”I de russiske nyhedsmedier og hacker-grupper har de skrevet, at de har ødelagt en masse offentlige tilbud i Estland. Men for at være ærlig har det store flertal af os i Estland ikke bemærket noget. Vi ville ikke ane, at vi var udsat for et cyberangreb, hvis ikke russerne havde fortalt os det.”

Den engelske forsker Dr. Adrian Venables fra Tallinns tekniske universitet, Center of software science, griner skævt over Skype-forbindelsen.

”Det var da vældigt pænt af dem, men det værste, som vi har set på de sociale medier, var, at man oplevede at skulle bruge to eller tre gange for at kunne betale med et kreditkort. Vi har i hvert fald ikke set noget, som kommer i nærheden af det, vi var udsat for i 2007.”

Den 27. april blev Estland ramt af et omfattende cyberangreb, der gik ud over det estiske parlament og ministerier. Også den private sektor – banker, aviser og tv-stationer – blev ramt af cyberangreb efter, at det blev besluttet at fjerne et mindesmærke for de sovjetiske soldater, en bronze statue af en soldat i sovjetisk uniform, fra hovedstaden Tallinns centrum til en militær kirkegård i udkanten af byen.

Stor indflydelse på samfundet

Mens mange fra det store russiske mindretal i landet så statuen som et vigtigt mindesmærke for sejren over Nazityskland, så et flertal i befolkningen tværtimod den som et symbol på den sovjetiske besættelse og undertrykkelse i årtierne efter den sidste verdenskrig.

”Cyberangrebet i 2007 fik stor indflydelse på samfundet her. Også selv om Estland kom sig forholdsvist hurtigt,” fastslår den britiske forsker.

Han fremhæver, at hovedparten af angrebene dengang var DDOS (Distributed Denial Of Service), hvor de estiske servere gik ned efter at være blevet bombarderet digitalt. Angrebet blev sporet tilbage til Rusland, hvor det officielle svar var, at det var privatpersoner, der havde reageret på den krænkelse, fjernelsen af statuen udgjorde.

”Rusland argumenterede med, at det ikke var en fjendtlig handling men derimod hærværk, som staten ikke havde noget ansvar for. Den argumentation er mere eller mindre påvist som falsk. Mange angreb kom fra regeringsbygninger og officielle IP-adresser, og de var godt koordineret som et af de første eksempler på den hybride krigsførelse, russerne senere har brugt meget; altså fjendtlige handlinger som Rusland ikke officielt står bag,” siger Adrian Venables.

Han henviser som et eksempel de såkaldte ”grønne mænd”, der blev anvendt til at angribe Ukraine i 2014. Nok talte de russisk og var udstyret med russiske våben, men Rusland ville ikke vedkende sig dem officielt. Ifølge vestlige analytikere var der dog tale om specialstyrker fra den militære efterretningstjeneste.

Konsekvensen af forløbet i 2007 har været, at de forskellige dele af det estiske samfund har forberedt sig på, at det vil være den måde, russerne vil angribe på:

”Siden Rusland invaderede Ukraine, var reaktionen i de baltiske lande den samme, nemlig at være klar til de russiske cyberangreb,” siger Adrian Venables.

Skattemyndighederne ramt

Efter Ruslands angreb på Ukraine i år bekendtgjorde den estiske regering, at andre anslået 200-400 sovjetiske mindesmærker til minde om anden verdenskrig skulle fjernes. Angrebet på Ukraine har åbnet de gamle sår fra den sovjetiske besættelse, lød det. Det mest omtalte har været, at et monument med en sovjetisk T-34 tank blev fjernet fra byen Narva i det østlige Estland, hvor godt 80 pct. af befolkningen er etnisk russisk.

”Så det var helt klart, at der ville komme en russisk reaktion. Så da den kom, var de estiske myndigheder klar til at modstå angrebet. Så vidt jeg er informeret, gik skattemyndighedernes hjemmeside ned i godt en time eller det, der ligner, men jeg tror ikke, at der var mange estere, som var så voldsomt bekymrede over, at det gik ud over lige dem.”

Han fortrækker næsten ikke en mine:

”Men den brede digitale infrastruktur, som er en normal del af et moderne samfund, var ikke berørt af de russiske angreb. De fleste, som gav deres mening til kende på de sociale medier mente, at der ikke var meget at bemærke. Men jeg er ikke i tvivl om, at der skjult for alles øjne blev arbejdet utroligt hårdt på at modgå angrebene. Der var sikkert mange nætter uden søvn i den kamp.”

”Faren for omfattende angreb var blæst op forinden. Man talte om faren for et digitalt Pearl Harbor, men det blev aldrig til virkelighed.”

Adrian Venables ser det som et tegn på, hvor modstandsdygtigt, det estiske samfund har formået at blive efter angrebene tilbage i 2007.

”Jeg synes også, at et godt tegn på dette har været, at den brede befolkning har kunnet begå sig normalt i hverdagen uden at skulle frygte, at den kritiske infrastruktur skulle gå ned, siger han.

Dog skal det med i en eftersætning, at mens der også var uroligheder og demonstrationer mod at fjerne bronzesoldaten i 2007, var protesterne fra det russiske mindretal langt mindre denne gang i 2022.

”Så i en vis forstand tror jeg også, at man kan sige, at Estland er kommet videre. Mens der er et stort russisk mindretal, bliver de ikke set som en femte kolonne i landet. Selvfølgelig vil der altid være ekstremister blandt dem, men flertallet er ikke ude på at ændre systemet. De kan se, at det er bedre at være en del af EU, at være på den her side af grænsen end at være på den russiske side.”

Trods alt en grænse for russernes formåen

Estland er ikke den eneste af de baltiske stater, som har fjernet sovjetiske monumenter. Adrian Venables henviser til, at også i Letlands hovedstad Riga fjernede man et større monument fra den tid, hvor

\ fortsættes side 27

> ”I de russiske nyhedsmedier og hacker-grupper har de skrevet, at de har ødelagt en masse offentlige tilbud i Estland. Men for at være ærlig har det store flertal af os i Estland ikke bemærket noget. Vi ville ikke ane, at vi var udsat for et cyberangreb, hvis ikke russerne havde fortalt os det.
>
> Adrian Venables.

man ikke i samme grad så en russisk cyber-gengældelse.
"Så man kan måske formode, at der er en grænse for, hvor mange denial-of-service-angreb, som Rusland er i stand til at gennemføre. Skal de angribe alle tre baltiske lande, vil det sprede angrebene ud over flere mål, hvad der gør dem mindre effektive," siger Adrian Venables.
Samtidig har det vist sig, at i hvert fald esterne er sværere at få has på.
Umiddelbart ser det ud til, at Estland har bestået den prøve, som de russiske cyberangreb har sat landets infrastruktur på. På trods af de voldsomme cyberangreb mod Estland tilbage i 2007, er der nemlig stadig en meget høj tillid til den digitale infrastruktur, hvad der med forskerens ord er fuldkommen essentielt for den samfundsmodel, esterne har opbygget, siden de genopstod som selvstændig efter Sovjetunionens sammenbrud.
I dag er Estland et land med en meget høj grad af digitalisering, hvor det bl.a. er muligt at stemme online til valg. Venables peger på, at også langt de fleste offentlige ydelser fås online.
"Det eneste, du ikke kan gøre fuldkommen online, er at købe fast ejendom og at blive gift eller skilt. Regeringen synes, at det egentlig ikke er en helt skidt ide, at hvis man skal giftes, skal man på et tidspunkt møde den udkårne fysisk," siger han.

Digital gennemsigtighed – begge veje

Mens den sidste bemærkning måske kan kalde på et smil, understreger den pointen om, hvor stor en grad af tillid, der er til systemet. I den sammenhæng kan Adrian Venables' beskrivelse af Estland minde meget om det danske samfund eller de øvrige skandinaviske lande, hvor tilliden er fundamentet for, at den digitale infrastruktur hænger sammen.
Som et eksempel understreger han, at den enkelte borger i Estland kan se, hvis en offentlig myndighed har søgt informationer om ham eller hende.
"Hvis jeg går ind på min personlige konto, kan jeg se, hvilke myndigheder der har haft adgang til mine data. De to undtagelser for den er efterretningstjenesten og, så vidt jeg ved også udlændingemyndighederne. Men hvis f.eks. politiet ser på mine data, kan jeg se det," siger Adrian Venables.
Denne gennemsigtighed i det offentliges adgang til personlige data er både med til at øge tilliden til systemet, og øge borgernes mulighed for at blive opmærksom på, hvis der er ubudne gæster, der har fået adgang til deres data. Bliver man opmærksom på en underlig trafik, kan man tage kontakt til myndighederne for at få svar på, hvorfor der bliver set på ens personlige data.
"Det minder om den måde, man anvender blockchain-teknologien, hvor der hele tiden bliver registreret, hvem der anvender de personlige data," siger Adrian Venables.

> Siden Rusland invaderede Ukraine, var reaktionen i de baltiske lande den samme, nemlig at være klar til de russiske cyberangreb.
>
> Adrian Venables.

RUSSISK INVASION HAR SYNLIGGJORT CYBERTRUSLEN

Da Putins tropper rullede ind i Ukraine forandrede det trusselsbilledet i store dele af verdenen.
Krigen har gjort mange flere opmærksomme på de risici, der følger med at have en digital infrastruktur i hackingens tidsalder.

"Invasionen af Ukraine fra Ruslands side er noget, der har påvirket hele det sikkerhedspolitiske billede. For så vidt angår cybertruslen, har den kun i begrænset omfang påvirket vores læsning af trusselsbilledet i Danmark. Det skal ses i lyset af, at når vi taler om cyberkriminalitet og cyberspionage, så har vi igennem længere tid kørt med et niveau, vi kalder 'meget højt' – det er det højst mulige niveau. Det betyder grundlæggende, sådan lidt firkantet sagt, at der er et meget, meget højt aktivitetsniveau. Trusselaktørerne, henholdsvis kriminelle og fremmede staters hackere, de kører døgnet rundt kampagner, hvor de forsøger at bryde ind i danske netværk og systemer. På den måde er det svært at få et højere aktivitetsniveau."
Ordene kommer fra Mark Fiedel. Han er chef for cyberanalyse-afdelingen i Center for Cybersikkerhed (CFCS) under Forsvarets Efterretningstjeneste. Han har indvilget i at sætte ord på det dagsaktuelle trusselsbillede for den digitale infrastruktur i Danmark, både den kritiske og den ikke-kritiske.

"Godt at nogen bliver forskrækkede"
Det er CFCS' vurdering, at invasionen af Ukraine ikke i sig selv har øget risikoen for, at danske interesser bliver udsat for hacking angreb.
"Vores vurdering er, at det sådan set har været et konstant højt niveau," siger Mark Fiedel.

\ fortsættes side 28

> Vi har haft rigtig, rigtig travlt. Allerede før invasionen var vi ude og advare om, at der kunne ske noget, og på den konto har vi haft virkelig, virkelig travlt. Det er en god ting. Vi får flere henvendelser, fordi man rundt omkring i organisationer bliver mere opmærksomme på, hvad det er, man skal kigge efter. Derfor reagerer man også oftere.
>
> Mark Fiedel

Når cybertrusler og hacking fylder mere, så er det altså ikke et udtryk for et øget trusselsniveau – som altså allerede før invasionen lå højest på CFCS' skala – men i stedet et udtryk for, at der er mere opmærksomhed på området.
"Invasionen har synliggjort nogle ting, hvilket betyder, at det er en kortere drøftelse, når vi skal forklare, hvorfor det er væsentligt at tage cybertrusler alvorligt. Det har forkortet de samtaler og den dialog, som vi har. Det har helt sikkert gjort noget i forhold til bevidstheden omkring cybertruslerne, og hvorfor man skal kigge på sin cyber-robusthed," siger han og fortsætter:
"Vi har også kunne se, og det var særligt tydeligt i både konflikten og senere krigens første faser, at der var en øget opmærksomhed rundt hos organisationer og også i private virksomheder, som betød, at man var meget hurtigere til at blive opmærksom på, når der skete noget. Man er blevet mere opmærksom på, at man skal kigge i sine logs og at man skal have logs, og at man rent faktisk skal holde øje med, hvad det er, der sker på ens netværk. Det betyder selvfølgelig også, at man reagerer på mere. Der er nogen, der er blevet forskrækkede. Det er faktisk rigtig, rigtig godt, at der er nogen, der bliver forskrækkede. For hvis man ikke har logs, så etablerer man logs og så begynder man at kigge på dem, og så kan man se, at man er under mere eller mindre konstant bombardement, hvor nogen forsøger at rekognoscere – altså forsøger at finde ud af "hvordan ser det ud?" med henblik på at bryde ind."

Travlhed og mørketal
Selvom antallet af angreb ikke ser ud til at være påvirket af invasionen, så har CFCS fået travlere.
"Der er mange, der henvender sig og siger: 'Det er meget værre nu, end det var før – der sker meget mere, end der gjorde før', men vores læsning er, at folk bare er mere opmærksomme," siger Mark Fiedel og fortsætter:
"Vi har haft rigtig, rigtig travlt. Allerede før invasionen var vi ude og advare om, at der kunne ske noget, og på den konto har vi haft virkelig, virkelig travlt. Det er en god ting. Vi får flere henvendelser, fordi man rundt omkring i organisationer bliver mere opmærksomme på, hvad det er, man skal kigge efter. Derfor reagerer man også oftere."
Han tilføjer, at der samtidig er mange angreb, der ikke bliver indrapporteret til CFCS:
"Jeg vil stadigvæk tro, at der er et rigtigt stort mørketal. Der er stadigvæk mange hændelser ud i både virksomheder, men også nogle myndigheder, som vi i virkeligheden ikke har noget visibilitet på, fordi vi ikke hører om det."

Mange angrebstyper
CFCS slås dagligt mod en bred vifte af angreb mod danske netværk, fortæller analysechef Mark Fiedel.
"Ransomware-angreb er klart den synligste og mest alvorlige trussel i vores optik. Det er ikke det samme, som at der kun sker ransomware-angreb, der er også CEO-svindel, hvor de kriminelle forsøger at svindle penge ud af organisationer ved f.eks. at udgive sig for at være fra ledelsen og beordre hastige pengeoverførsler. Det kan være rigtig kritisk for den enkelte virksomhed, men vores fokus er jo også på, hvad det betyder for samfundet. Vi er sat i verden for at bidrage til at imødegå cyber-trusler, særligt mod statslige myndigheder, forsvar og kritisk infrastruktur. Ransomware-angreb rammer ikke kun den enkelte virksomhed eller organisation, men kan også have negative konsekvenser på forsyningssikkerheden, for eksempel strøm eller vand."
Han fortæller, at angrebsmetoderne både tæller "håndholdte", manuelle angreb og de helt automatiserede indtrængingsforsøg.
"Der er grundlæggende to forskellige typer, jeg vil fremhæve. Der er phishing-forsøg, hvor de kriminelle sender mails ud og håber, at der er nogen, der klikker på en vedhæftning eller et link, som så kører noget ondsindet kode. Det er den ene kategori. Den anden, kører nærmest døgnet rundt i industriel skala, også mod danske netværk. Det er automatiserede forsøg på bruteforcing og på at udnytte kendte sårbarheder i software på f.eks. mailservere. Det er desværre let for hackerne, både de kriminelle og de statslige hackere, at automatisere de her angrebsforsøg. De laver grundlæggende et lille program, som de sender ud på nogle maskiner, og så står maskinerne bare og rundérer internettet døgnet rundt."

En trussel, der er kommet for at blive
Mark Fiedel og CFCS' vurdering er, at cyberkriminalitet ikke bare er et modefænomen. Det er kommet for at blive, og det er en konstant kamp om at være et skridt foran modstanderen.
"Det er jo et kapløb mellem angribere, som udvikler deres forretningsmodel og deres værktøjer, og så forsvarerne – sådan nogle som os, og dem der sidder ude i virksomheder og myndigheder – der hele tiden skal forsøge at hæve barren for, hvor dyrt det er for angriberen at komme ind," siger han.
Når virksomheder eller myndigheder angribes, så kan angribernes motiver være meget forskellige. Mange er kriminelle, der er motiveret af jagten på penge, mens andre angreb kommer fra statslige aktører.
"Vi deler de forskellige trusler op efter motiverne, og de to mest alvorlige – cyberspionage og cyberkriminalitet – forsvinder jo ikke. Spionage-elementet forsvinder ikke i forudsigelig fremtid. Kriminalitet ej heller. Det forsvinder først, når folk holder op med at ville stjæle fra hinanden, og der går nok en rum tid. Så længe vi er digitaliserede, så længe vi er afhængige af digitale tjenester, så vil det også være noget, der bliver forsøgt udnyttet.

> Ransomware-angreb rammer ikke kun den enkelte virksomhed eller organisation, men kan også have negative konsekvenser på forsyningssikkerheden, for eksempel strøm eller vand.

Ikke hvorvidt, men hvornår
Han understreger flere gange, at CFCS' primære budskab er, at alle er i risikozonen, og at det først og fremmest er et spørgsmål om, hvordan man håndterer et angreb, ikke hvorvidt man bliver angrebet.
"Det er ikke et spørgsmål, om hvornår 'man bliver forsøgt ramt'. Det er et spørgsmål, om når man bliver forsøgt ramt. Det er vigtigt, at man har haft en risikovurdering som udpeger de mest sårbare dele, og at man har iværksat de beskyttelsesforanstaltninger, som man har vurderet er passende," lyder det fra Mark Fiedel.
Han uddyber:
"Det er både som organisation i forhold til tekniske foranstaltninger, men også de interne processer, medarbejderne og bevidstheden omkring truslen. Er der en sikkerhedsorganisation internt? Hvis man bliver ramt, har man så styr på det? Hvem tager kontakt til myndigheder? Har man en beredskabsplan, der ikke ligger på det drev, der eventuelt måtte blive ramt? Har man alternative kommunikationskanaler, hvis ens mail bliver ramt? Hvordan kommunikerer man så med leverandør og sin egen organisation? Alle de spørgsmål bør man have besvaret før angrebet finder sted."
Og ikke nok med det, så bør man også have en plan for at komme på fode igen bagefter:
"Er man i stand til at reetablere sig selv? Har man en backup, der virker, og som man er trænet i at reetablere? Har man sin kontakt til sikkerhedsleverandøren ift. både at håndtere den konkrete hændelse, men også at kunne hjælpe med at komme på fode igen? Det er i virkeligheden hele kæden, man skal have taget stilling til."

BLIV SKARPERE – KURSER OG ARRANGEMENTER

Som medlem af HK kan du melde dig til alle de arrangementer og kurser, du vil – uden at det koster dig andet end din tid.
Så kan du både styrke dine kompetencer, deltage i debatter og få masser af inspiration.

ONLINEKURSER

Velkommen til SAMDATA\HKs univers af onlinekurser.
Her kan du dygtiggøre dig, når du har tid og lyst og i dit eget tempo.
Se kurserne nedenfor.

IT-SIKKERHED OG DATABASE

- Cloud-databaser for begyndere
- Din personlige IT-sikkerhed
- NoSQL
- Sikkerhed og kryptering
- SQL

ANDET

- Introduktion til Microsoft Teams
- Studieteknik på videregående uddannelser
- Wordpress

JEPPE ENGELL ER IT-FAGLIG KONSULENT I SAMDATA\HK OG DEN DAGLIGE LEDER AF SAMDATA\HK SEKRETARIATET

Har du spørgsmål, gode ideer, kritik eller ønsker, så hold dig ikke tilbage fra at kontakte Jeppe:

MOBIL +45 40728990
jeppe.engell@hk.dk
dk.linkedin.com/in/engell/
twitter.com/jeppeengell

\ FIND MERE INFO OM SAMDATA\HK PÅ

HAR DU SPØRGSMÅL?
SEND EN MAIL TIL: SAMDATA@HK.DK

CERTIFICERING

- 93011 Windows Server 2019 Administration
- 96040 Managing Sharepoint and OneDrive in Microsoft 365
- Administration af Windows Server 2012 - (70-411)
- Avanceret konfiguration af Windows Server 2012 - (70-412)
- AZ-104 - Introduktion til AZ - Bliv Azure administrator
- Enabling Office 365 Services (70-347)
- Implementering Microsoft Azure Infrastructure Solutions (70-533)
- Installering og konfiguration af Windows Server 2012 - (70-410)
- MCP 120035 Introduktion til Microsoft Power Automate
- MD 101 Managing Modern Desktops
- Microsoft Azure Infrastructure and Deployment (70100)
- Microsoft Azure Integration and Security (70101)
- Microsoft: Installing, Maintaining and Protecting Windows 10
- PL-100 Microsoft Power Platform App Maker
- PL-900 Microsoft Power Platform Fundamentals
- PowerShell
- SCCM - Administrering System Center Configuration Manager
- SCOM - Administrering System Center Operations Manager

PROGRAMMERING

- App-udvikling i C#
- Bash - Linux scripting
- Blazor for begyndere
- C# - Grundkursus 1
- C# - Grundkursus 2
- C# programmering med Michell Cronberg
- Dataanalyse i Python
- HTML og CSS
- Jave - Grundkursus 1
- JavaScript og jQuery
- Machine learning i Python
- Overblik over grundlæggende webudvikling
- PHP
- Python - Grundkursus 1
- Python - Grundkursus 2
- RESTful webservices i.NET Core med C#
- Visuel programmering for begyndere
- WebAssembly

\ LÆS MERE OM KURSERNE PÅ
HTTP://KORTLINK.DK/2G9BG

SAMDATA \ IT-FAGETS FAGFORENING \ HK

\ Af Andreas Rasmussen, ar@andreas-rasmussen.dk

"DET ER MERE INTERESSANT AT BESKYTTE END AT ANGRIBE SYSTEMER"

Der er mange karrieremuligheder, hvis man arbejder med IT-sikkerhed. En af dem, der prøver dem af, er Lea Gemzøe Nielsen.

I august startede Lea Gemzøe Nielsen på top up-uddannelsen i IT-sikkerhed på Københavns Erhvervsakademi.

"Jeg vil gerne vide, hvordan de systemer, som vi allesammen bruger, fungerer, og hvordan vi kan beskytte dem, for angreb forekommer oftere og oftere," fortæller hun.

Før sommerferien blev hun færdig med den to-årige uddannelse som IT-teknolog, der også foregik på KEA. Den handler især om netværk, programmering og Internet of Things, IoT,altså dét fænomen, at flere og flere genstande nu er koblet på internettet.

Ved efterfølgende at bruge halvandet år på IT-sikkerhed får hun samlet set en professionsbachelor.

"Jeg valgte faktisk at tage IT-teknolog-uddannelsen for efterfølgende at kunne tage uddannelsen i IT-sikkerhed," forklarer hun.

Den 27-årige sikkerhedsstudent blev i første omgang overrasket over hvor frit spil cyberkriminelle har:

"Der, der fascinerede mig var, hvor let det var, og hvor stor en rolle mennesker spiller i det. Den største risiko hos virksomheder er menneskerne, der abejder dér, fordi de klikker på farlige links eller har dårlige passwords," siger hun og fortsætter:

"Men jeg synes klart, at det er mere interessant at beskytte end at angribe systemer. På IT-teknolog-uddannelsen begyndte jeg at interessere mig for hackingdelen, altså den offensive del. Men så fik jeg øjnene op for den defensive del, dét, der også kaldes blue teaming."

For hende er det ikke kun et spørgsmål om det tekniske aspekt, men også det menneskelige.

"Det der er spændende er at beskytte selve systemet, men også at arbejde med awareness; at oplyse medarbejderne om, hvordan man håndterer bestemte situationer."

Blandt andet derfor er hun glad for at være startet på den nye uddannelse:

"Vi skal blandt andet arbejde med GDPR og IT-governance, så man får redskaber til at give information videre til medarbejderne," lyder det fra Lea Gemzøe Nielsen.

Hun har ikke et bestemt mål for sin karriere, for "der er så mange døre, at det er svært at vide, hvor man ender henne, før man er der", som hun siger. Hun har dog allerede et studiejob i efterretningsvirksomheden Certa Intelligence & Security, der er stiftet af den tidligere PET-chef Jakob Scharf.

Men selvom hun allerede er i gang med IT-uddannelse nummer to og har et relevant studiejob, så er hun langt fra færdig med at blive klogere.

"Vi lærer at opsøge viden og at kunne sætte os ind i ny viden hurtigt. Det er en branche, hvor man aldrig stopper med at skulle lære. Der er konstant noget, der ændrer sig. Man kan ikke tage en IT-uddannelse og så sige 'nu skal jeg ikke lære mere'. Det giver ikke mening."

Lea Gemzøe Nielsens bedste råd til andre studerende er at have tålmodighed.

"Man skal hænge i, især i starten. Der er rigtigt meget, der ikke giver mening, hvis man ikke har arbejdet med IT før. Men lige pludselig så åbner hele verdenen sig for en, og så giver det hele mening. Hæng i og hold ud."