Ændrer vi ikke vaner, kommer vi aldrig i mål med cybersikkerheden

Vores modvilje mod at ændre indgroede digitale vaner er en af de største udfordringer for cybersikkerheden – både for den enkelte dansker og for samfundet, vurderer lektor i statskundskab Morten Brænder.

Jeppe Kyhne Knudsen, Aktuel Naturvidenskab.

Du kender det nok. Du er blevet logget ud af en af de utallige digitale tjenester, du bruger – og nu kan du ikke huske kodeordet. Vi skal efterhånden logge ind de fleste steder, og de færreste af os kan huske hundredvis af forskellige koder. Derfor bruger vi de samme få kodeord.

Du forsøger dig derfor med en af de sædvanlige koder – og det virker. Du havde genbrugt en gammel traver.

Men det er ikke en god ting, fortæller lektor Morten Brænder.

»De fleste af os ved jo godt, at vi burde bruge en password-generator til at lave sikre kodeord. Men dem kan vi ikke huske, og det bliver for besværligt. I stedet bruger vi de samme få kodeord igen og igen.«

Dårlige kodeord er bare et eksempel på, hvor svært det er at ændre vaner. En anden er at skifte til de programmer, som virksomheden eller organisationen af sikkerhedshensyn anbefaler.

»Her på Aarhus Universitet anbefaler it-afdelingen, at vi bruger Microsoft-løsninger, fordi vi har en sikker databehandlingsaftale med dem. Det gælder også i forhold til fildeling. Men hvis man har vænnet sig til at bruge for eksempel DropBox eller Google Drive, er det virkeligt fristende at blive ved med det, fordi det simpelthen er for bøvlet at skifte, eller fordi disse løsninger er mere driftssikre. Giver man efter for den fristelse, slækker man på sikkerheden. Det er menneskeligt at lade vanen styre. Men vanen kan nogle gange føre til, at vi gør det modsatte af, hvad vi bliver påbudt at gøre.«

Psykologerne kalder fænomenet for revenge-effekten. Tiltag som egentlig skal styrke sikkerheden, ender med at forringe den. Det er blevet for besværligt at skifte, så derfor nægter vi.

Når EU-regler spænder ben for forskningen

I EU er vi meget opsatte på at lave regler og skabe digital sikkerhed. Men heller ikke på organisationsniveau er det sikkert, at den slags tiltag virker efter hensigten, forklarer Morten Brænder.

»I forsknings- og administrationskredse er det meste berygtede tiltag nok GDPR og alle de ressourcer, det har krævet at implementere. I mange virksomheder taler man i dag om NIS2-direktivet, som fra 2025 bliver implementeret i Danmark, og som skal sikre EU's cybersikkerhed i en tid med hybridkrig og stigende trusler fra hackere. Den slags standarder har vi masser af i EU. De kan være en virkelig god ting. Dels fordi de forhåbentlig øger sikkerheden for os alle. Dels fordi det ofte ender med, at andre lande tilpasser sig vores standarder,« siger Morten Brænder.

»Udfordringen er bare, at det er ret forskelligt, hvordan organisationer tilpasser sig. GDPR betyder ikke det samme i Danmark som i andre lande, og selv på Aarhus Universitet har jeg oplevet at få helt modsatrettede råd i forhold til håndtering af personfølsomme data på tværs af fakulteterne. Dertil kommer, at man som forsker nogle gange kan føle, at man spiller Ludo og hele tiden bliver slået hjem. Man skal have ekstremt mange tilladelser for at bruge personfølsomme data til forskning. Spørgsmålet er altså, om direktiverne virker efter hensigten. Både på individ-niveau og i store organisationer, er man nemlig ikke bedre end det svageste led i kæden.«

Set fra et rent sikkerhedsperspektiv handler det om, at medarbejderne skal følge de procedurer, som bliver fastsat. Der skal ikke mere end én medarbejder med dårlige vaner til, før det hele kan vælte.

»Men tager vi et skridt tilbage, handler sikkerhed ikke kun om teknologi eller procedurer, men også om, at vi forholder os til betydningen af menneskelige og sociale faktorer. For hvis oplevelsen af procedurerne er, at de kun gør det både dyrere og mere besværligt for alle, risikerer vi at undergrave den tillid, der kan rette op på disse vaner,« siger Morten Brænder.

En skrøbelig situation

Fingeren peger derfor ikke udelukkende på individer med dårlig IT-sikkerheds-hygiejne. Der er også nogle politiske beslutninger, og vi skal spørge os selv, om nogle af vores overordnede infrastrukturløsninger har gjort os for skrøbelige, vurderer Morten Brænder.

»For tre år siden boede jeg i Ohio. Skal man med en bus der, har man fire muligheder for at betale. Et system, der minder om rejsekortet, et universitetskort, ens kreditkort eller kontanter. Fire systemer, der skal bryde ned, for at man ikke kan tage bussen. Det er resiliens,« fortæller Morten Brænder og fortsætter:

»I Danmark har vi kun én digital infrastruktur tilbage omkring offentlig transport. Du kan ikke være sikker på at kunne betale kontant i busserne længere, klippekortet er afskaffet, og det fysiske rejsekort er på vej ud. Men forlader vi os på et begrænset antal løsninger kræver det også et begrænset angreb på ét system og en hel sektor er sat ud af spillet. Det er ikke resiliens.«

En ting er transport, noget andet er den virkelig kritiske infrastruktur, for eksempel el- og vandforsyning.

»Lukker du for et sygehus' vandforsyning, tæller vi ikke dage og formentlig ikke engang timer, før tingene bliver virkelig alvorlige.

AU Foto

Morten Brænder

Han er lektor i statskundskab på Aarhus Universitet og sidder i ledelsesgruppen i Kong Frederiks Center for Offentlig Ledelse med ansvar for forsvar og beredskab.
Hans primære forskningsområder omfatter militærsociologi, motivation, ledelse og rekruttering i Forsvaret.

REVENGE-EFFEKTEN

I 1997 udgav videnskabshistorikeren Edward Tenner bogen *Why Things Bite Back: Technology and the Revenge of Unintended Consequences.* Heri fandt han på begrebet revenge-effekt.

Hans pointe er, at ny teknologi ofte hævner sig ved at skabe det præcis modsatte resultat af, hvad der oprindeligt var hensigten. Eksempelvis skulle computer og emails gøre papiret overflødigt og begrænse skovfældning, men i stedet blev det nemt at printe og papirforbruget eksploderede – i hvert fald i en årrække.

I forhold til cybersikkerhed er hensigten med svære adgangskoder, to-faktor-godkendelse og krav om hele tiden at skifte password at gøre en virksomhed eller organisation mere sikker. Men fordi det er besværligt, ender det ofte med det modsatte.

Folk sætter post-its med koder på skærmen eller gemmer alle deres passwords i et dokument og ender altså med at gøre virksomheder endnu mere usikre. I stedet skulle de måske beholde deres mindre sikre passwords.

Vand er ikke blot afgørende for at folk får væske, men også for hygiejnen. Når vi bygger nye supersygehuse, skal vi derfor ikke blot være sikre på, at der er adgang til vand, men også at de systemer, der værner om forsyningen heraf, er sikret mod for eksempel cyberangreb,« siger Morten Brænder.

En ny form for værnepligt?
Ifølge Morten Brænder var det mest interessante ved den panik, der opstod den 23. september 2025 ikke spørgsmålet om, hvorvidt der var droner over Københavns Lufthavn. Det mest interessante var, at situationen med al tydelighed viste, hvor let det er at få os til at kigge i én bestemt retning. Forsvarets ledelse skal helt sikkert tage droner alvorligt i deres indkøbspolitik. Men i fredstid er den skade, droner kan forventes at forårsage, ret begrænset sammenlignet med konsekvenserne af et nedbrud af vand eller elforsyningen.

»Problemet er, at ingen rigtig interesserer sig for cybersikkerhed. Det er ikke fysisk og konkret ligesom nye krigsskibe eller F-35-fly, selvom det ud fra et samfundsperspektiv er mindst lige så vigtigt,« siger Morten Brænder.

»Vi er enormt sårbare over for cybertruslen. Udover at der mangler eksperter på området, er et af de store problemer, at vores generelle viden herom er begrænset, og at vores i øvrigt meget velfungerende digitaliserede samfund gør os afhængige af løsninger, der netop også kan angribes digitalt.«

»Årgangene er små, og selvom flere skulle søge ind på IT-uddannelserne, er det spørgsmålet, hvor meget det vil flytte. Så hvad gør vi?« siger Morten Brænder.

Han påpeger, at Forsvaret allerede har et cyberværnepligt-spor, men optaget er ret begrænset, og at den viden de unge værnepligtige tilegner sig, derfor vil få en begrænset udbredelse.

»Men tanken om, at en større andel af befolkningen kan deltage i Danmarks digitale forsvar gennem en "cyberværnepligt", er måske ikke helt skæv. Det er dog i sidste ende en politisk beslutning, og det allervigtigste i den sammenhæng er nok, at vi som samfund sikrer, at det fælles ansvar for vores digitale sikkerhed ikke opleves som en hæmsko. Ikke mindst i det lys er vi nødt til at have en debat om cybersikkerhed i Danmark. Ellers sker der intet. Ligesom med klimadagsordenen ved vi, at det kan tage mange år, fra forskningen erkender et problemet, til der rent faktisk begynder at ske noget,« slutter Morten Brænder. ■