Cyber-kriminalitet:

Lav moral og litt startkapital

Det er alt som trengs for å starte som cyber-kriminell i dag. Angrepsverktøy, adresselister, e-postutsendelser, utpressings- og hvitvaskingstjenester – alt er tilgjengelig for den som mangler moralske sperrer og kan avse noen bitcoins.

Director
Chris Culina
Leder BDO Cybersecurity

Risikoen for å bli tatt er lav. Så lav at det for noen kan virke legitimt. Enkelhet, tilgjengelighet, høy avkastning og lav risiko gjør at stadig flere kaster seg på bølgen, og profiterer på den lave sikkerhetsbevisstheten i samfunnet.

Et lovløst lykkeland

Datakriminalitet har utviklet seg fra en eksklusiv klubb bestående av eksperter og nasjonalstater til et lovløst lykkeland for opportunister. Denne utviklingen har medført en endring i trusselbildet i retning av det kaotiske. Bredden blant trusselaktørene gjør at motivasjonen er variert og Internetts grenseoverskridende natur gjør at geografisk lokasjon har liten betydning. Kort oppsummert: Alle har digitale verdier som er interessante for noen, og en motivert trusselaktør kan med lav kostnad og risiko ramme verdiene fra hvor som helst i verden, når som helst.

Bli mer årvåken

For deg og meg betyr dagens digitale risikobilde at vi må bli mer årvåkne. Personlig informasjon, familiebilder, viktige dokumenter og økonomiske transaksjoner – hele livet og familien på nett. Privatpersoner blir utsatt for utpressing og sjikane, mister uerstattelige familieminner, blir svindlet, fratstjålet penger og utsatt for identitetstyveri.

Når man tenker etter, er det en litt underlig utvikling. Få av oss hadde villet henge opp familiebilder på oppslagstavla til velforeningen, men mange av oss synes det er helt greit å dele det samme via sosiale medier. Få av oss hadde sendt kontanter til en ukjent butikk på et annet kontinent, men mange av oss handler bekymringsløst i nettbutikker verden over. Fra hjemmets trygge sofakrok virker truslene langt unna.

For rask utvikling

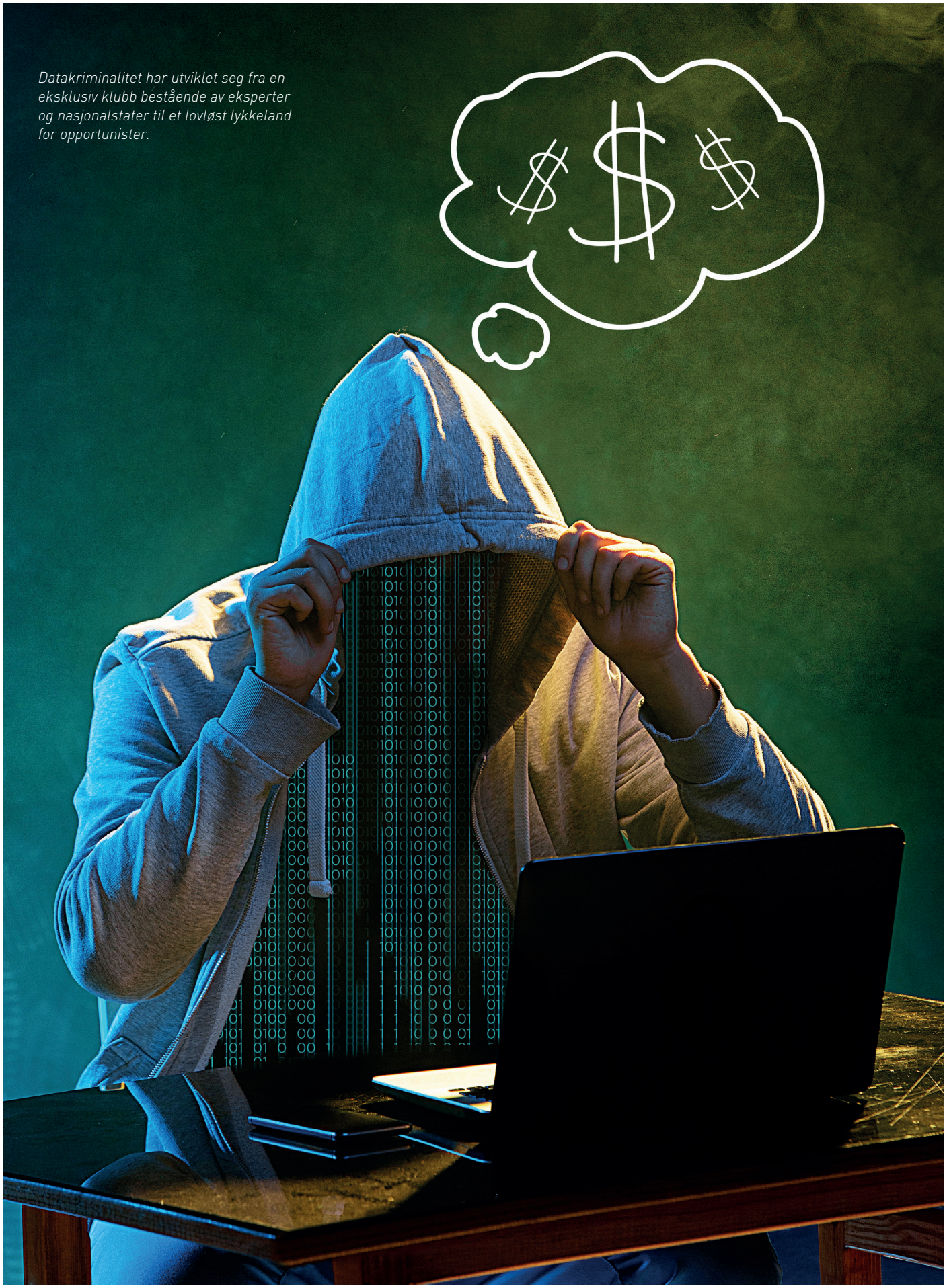
Er det noe med mediet? Tastaturet skaper en trygg distanse til truslene, også på det emosjonelle planet. Tenk bare på hvor villig mange er til å stole på mennesker via tastaturet, selv uten å ha sett eller møtt dem. Nettdating kan være et godt eksempel på dette. Risikoforståelsen vår bygger på empiri, og stort sett er vi ganske flinke til å gjøre risikovurderinger i hverdagen. Det ser litt grått ut, så jeg tar med en paraply. Trappen er bratt, så jeg holder meg i rekkverket. Gulvet er vått, så jeg antar det er glatt. En ungdomsgjeng plager en person på T-banen – skal jeg gripe inn eller ringe politiet? En stor del av problemet ligger i at empirien vår kommer fra den fysiske verden. Mye lar seg overføre til den digitale, men ikke uten videre. Utviklingen har kanskje skjedd for fort.

Identifiser verdiene

Også virksomheter, både offentlige og private, står overfor de samme utfordringene. Vi tar med oss risikoforståelsen inn i jobbene som arbeidere, ledere, kontrollører og rådgivere. I tillegg til lav trusselforståelse, har mange virksomheter problemer med å peke på verdiene sine. Det er ikke få ganger jeg har hørt ledelsen hevde at virksomheten ikke har verdier som trenger beskyttelse, rett etter at de har blitt utsatt for et alvorlig dataangrep. Verdivurdering, som i denne sammenheng betyr vurdering av skadepotensialet knyttet til verdiene, er sentralt i risikovurderingen, men umulig å gjennomføre hvis man ikke evner å identifisere verdiene.

Kartlegg verdiene

Alt som berører IT og har betydning for virksomheten, må regnes som digitale informasjonsverdier. Listen er sannsynligvis lang. Hyppig forekommende verdier inkluderer omdømme, operativ evne, personopplysninger, kundedata, know-how, produksjonsmetoder, markedsstrategier, forskning



Datakriminalitet har utviklet seg fra en eksklusiv klubb bestående av eksperter og nasjonalstater til et lovløst lykkeland for opportunister.

og utvikling, kontraktsforhandlinger, konkurransefortrinn, sikkerhetsgradert informasjon, informasjon om kritisk infrastruktur, relasjoner til andre virksomheter med verdi, produksjonssystemer, kommunikasjonsløsninger, websider, sosiale medier, kundedatabaser, saksbehandlingssystemer og finansielle verdier – for å nevne noen. Om du ikke gjør kartlegging og vurdering av dine egne verdier, kan du iallfall være sikker på at noen der ute gjør det. Så gjenstår det å se hvor motivert de blir.

Vanskelig å oppdage

Det er selvsagt ikke sikkert du noen gang finner ut hvor motivert noen ble av verdiene dine, og om du finner det ut, kan det godt være for sent. Visse typer dataangrep er det umulig å ikke oppdage, f.eks. utpressing som baserer seg på å kryptere filene dine. Spionasje, eller andre former for informasjonstyveri, kan godt tenkes å passere under radaren.

I vår fysiske verden innebærer tyveri normalt at noe blir borte. At vinduet er knust og smykkene forsvunnet, er et godt tegn på at du har hatt innbrudd. Når inntrengere forsyner seg av sensitiv informasjon på datamaskinen din, blir ingenting borte. Det gjør det vanskeligere å oppdage tyveriet.

Utnytter sårbarheter i systemene

Dessverre finnes det ingen enkel løsning på problemet med digital kriminalitet. Det finnes ingen tiltak som gjør oss helt sikre. For å nå verdiene utnytter trusselaktører sårbarheter i systemene våre. Sårbarhetene kan være menneskelige, organisatoriske og teknologiske. En ansatt som kan lures til å utlevere sensitiv informasjon, utgjør en menneskelig sårbarhet. Sviktende rutiner for godkjenning av utbetalinger kan utgjøre en organisatorisk sårbarhet. Et dårlig konfigurert e-postsystem, som ikke filtrerer bort forfalsket e-post, representerer en teknologisk sårbarhet. Trusselaktøren utnytter disse i tur og orden. Ved å forfalske direktørens e-postadresse, lurer han en ansatt til å overføre penger til utlandet. På grunn av mangelfulle rutiner for verifisering av utbetalinger, får offeret overføre penger uten at svindelen oppdages før det er for sent og pengene er tapt.

Ukjente sårbarheter

Teknologien bringer også med seg et annet problem, nemlig ukjente sårbarheter. Vi er vant til å kunne støtte vurderinger og beslutninger på direkte observasjoner. Det kan vi ofte ikke med programvare og IT-systemer. Programvaresårbarheter kan være skjult i lang tid før de oppdages – ofte av noen andre enn produsenten. Det er faktisk virksomheter og enkeltpersoner som har spesialisert seg på å finne sårbarheter i programvare, for så å selge informasjon om sårbarhetene til trusselaktører. At vi vet så lite om vår faktiske sårbarhet, fører til at risikovurderingene må ta høyde for en viss usikkerhet. Vi kan simpelthen ikke vite sikkert. Vi må ikke la oss lede til å tro at

mangel på kunnskap om sårbarheter betyr mangel på sårbarheter.

En balansert tilnærming

Hvis man forsøker å sikre alt maksimalt, vil en raskt oppdage at sikkerhet koster mer enn det smaker. Det blir sannsynligvis også åpenbart at man ikke kommer helt i mål, og at man på veien har gjort det vanskelig å få gjort jobben. Sikring må være balansert. Tenk på sikkerhet som lagvise tiltak, hvor hvert enkelt tiltak ikke nødvendigvis skal hindre alt, men bidra til å redusere risikoen for tap av verdier. Den balanserte tilnærmingen skal sørge for at tiltakene settes inn der de gir størst effekt – der de største verdiene og det største skadepotensialet er.

Lett å gjøre en feilpasning

Digitaliseringen som pågår, medfører mye bra. Vi ser økt effektivisering, utnyttelse av eksisterende teknologi på nye måter, og en slags demokratisering av markedet, hvor en liten virksomhet med en god idé har større muligheter til å nå et globalt marked og konkurrere med store, etablerte aktører. Skyggesiden av digitaliseringen er at vi gjør oss stadig mer avhengige av digitale løsninger, uten at sikkerhet og robusthet gis nok oppmerksomhet. Dette er som å spille ballen rett til de kriminelle.

Tre gode spørsmål

1. Har virksomheten digitale informasjonsverdier?
2. Har virksomheten et styringssystem for informasjonssikkerhet?
3. Har man KPI-er på informasjonssikkerhet?

Må forankres i virksomhetsstyringen

Vi kan endre ligningen, og gjøre datakriminalitet mindre attraktivt. Det gjør vi ved å redusere sårbarhetene og bedre evnen til å oppdage uønsket aktivitet, for på den måten å øke kostnaden og risikoen til de som tjener penger på datakriminalitet. Hvem skal sørge for dette? IT-avdelingen? De ansatte? Når vi ser at manglende sikkerhet kan ødelegge omdømmet til en virksomhet, eller i løpet av sekunder føre til at viktige konkurransefortrinn tapes, skjønner vi at sikkerhetsrisiko er en del av virksomhetsrisikoen. Følgelig må sikkerhetsstyringen forankres i virksomhetsstyringen, hos dem som til syvende og sist eier risikoen.

Revisors spesielle rolle

Revisor har en spesiell rolle som kontrollør og rådgiver, og forholder seg naturlig til virksomhetsrisiko. Når revisor ser at virksomheten har digitale avhengigheter, bør risikovurderingene også ta hensyn til digital sikkerhetsrisiko. Ukentlig blir vi minnet på risikoen av mediene, som stadig bringer oss siste nytt om svindel, utpressing, spionasje og sabotasje. Dette gir gode anledninger for revisor til å stille spørsmål. Du trenger ofte ikke å være sikkerhetsekspert for å hente verdi ut av svarene – nøling og flakkende blikk forteller nok.