OPINION

Dette er et debatindlæg. Indlægget er udtryk for skribentens holdning. Alle holdninger, som kan udtrykkes inden for straffelovens og presseetikkens rammer, er velkomne, og du kan også sende os din mening her.

"Kære topledelser, jeres cybersikkerhedsfolk mangler retning"

"Rygraden i enhver god cybersikkerhedsstrategi er at foretage en bred risikovurdering," skriver indlæggets afsendere. Arkivfoto: Gleb Garanich/Reuters/Ritzau Scanpix
Foto: Scanpix Denmark

BO DREJER, GRC-MANAGER, ORANGE CYBERDEFENSE DANMARK
FRANS SKOVHOLM, ADVOKAT OG PARTNER, DAHL ADVOKATPARTNERSELSKAB

22. OKT. 2024 KL. 11.00 DEL GEM TIL SENERE

Når det gælder cybersikkerhed, tøver mange topledelser stadig med at tage styringen. Det er en skam, for det handler ikke om at forstå indviklet teknik, men om klassisk risikovurdering

I vores arbejde er vi så heldige at møde mange virkelig kompetente topledere. Men selv for dem kan cybersikkerhed være en blind vinkel.

Argumentet lyder ofte noget i retning af: "Jeg ved jo ikke noget om firewalls og hacking og kryptering – det er vel derfor, vi har en hel afdelingen med it-folk?"

Både ja og nej. For i takt med af it bliver stadig mere forretningskritisk, rykker ansvaret automatisk tættere på direktionsgangen og bestyrelseslokalet.

Smart bliver det også alvor i juridisk forstand. Når EU-direktiver som NIS2 og CER implementeres i dansk lovgivning, står mange ledelser med det endegyldige sikkerhedsansvar – uanset om de bryder sig om det eller ej.

Så hvordan griber man bolden og får det bedste ud af den udvikling? Her kommer nogle råd.

Tag ejerskab

Rygraden i enhver god cybersikkerhedsstrategi er at foretage en bred risikovurdering. Hvilke af jeres forretningsservices er vigtigst? Og hvilke dele af jeres it understøtter dem?

Hvad kan I tåle at miste, og hvad må I absolut ikke tabe kontrollen over, hvis jeres kerneforretningen skal kunne køre under ethvert cyberangreb? Og hvad med jeres kunder og partnere? Hvor har de behov for, at I prioriterer sikkerheden ekstra højt?

Dette er klassisk risk management, som helt naturligt hører hjemme på direktionsgangen. Husk på, at de fleste it-folk er teknologidrevne.

De tænker og agerer primært i forhold til teknologi. De interesserer sig i mindre grad for abstrakte risikovurderinger, som de reelt set ikke har ansvaret for. Deres fokus er typisk rettet mod konkrete prioriteringer, og hvad der skal bygges hvornår og hvordan.

Hvis I som ledelse stikker hovedet i sandet og overlader strategiopgaven til dem, vil de naturligvis gå efter at løse den, så godt de overhovedet kan.

Men det kan nemt føre til overbeskyttelse og unødvendige ekstraomkostninger. Især fordi de ikke er fortrolige nok med, hvilke risici der faktisk er acceptable, og derfor vælger at bygge med livrem og seler hele vejen igennem.

En afbalanceret risikoprofil

Overbeskyttelse kan måske lyde trygt. Men det er det ikke, for ingen har ubegrænsede ressourcer, og alle mangler it-specialister.

Derfor er det bedre og ofte billigere at skabe et helstøbt cyberforsvar, der nøje afspejler jeres reelle sikkerhedsbehov, så panseret gøres tykkest, hvor sårbarheden er størst. Det er vejen til maksimalt afkast på jeres sikkerhedsinvesteringer.

I den sammenhæng er det vigtigt, at I som ledelse er jeres risikoanalytiske rolle bevidst, og det er naturligvis også en del af forklaring på, hvorfor mere og mere lovgivning skubber ansvaret jeres vej.

Det betyder ikke, at I behøver at forstå, hvordan jeres digitale værdier skal beskyttes rent teknisk, men at I bruger jeres risikoanalytiske kompetencer til at udpege, hvad der skal beskyttes med alle midler, men også hvor I godt kan leve med en vis risiko.

> Overbeskyttelse kan måske lyde trygt. Men det er det ikke, for ingen har ubegrænsede ressourcer

Jo bedre I er til at kommunikere de rette sikkerhedsbehov, jo bedre kan it-afdelingen eller jeres sikkerhedspartnere træffe de optimale taktiske valg.

Som ledelse bør I således påtage jer en mere udførende rolle, hvor I vurderer og udfordrer jeres sikkerhedsbehov i en mere forretningsnær kontekst.

Over tid vil I kunne bevæge jer mere og mere frit i snitfladen mellem jeres risikoprofil og det operationelle sikkerhedsarbejde. Alt tyder på, at virksomheder, hvor ledelsen aktivt involverer sig i at tegne den rette risikoprofil, foretager mere hensigtsmæssige investeringer i cybersikkerhed.

Undervurdér ikke jeres egen viden

Bottom line er, at set i et ledelsesperspektiv er it ikke det mystiske og indviklede driftsområde, som giver mange ledelser berøringsangst.

Føler man det, er det fristende at bestille kostbare analyserapporter, som ofte er svære at omsætte til konkret sikkerhed, når konsulenterne har trukket sig tilbage.

Det virker måske udfordrende at tage mere styring på et område, der aldrig før har været på agendaen hos direktion og bestyrelse. Men ingen kender forretningen bedre end jer, og den viden er guld værd i forhold til jeres cybersikkerhed.

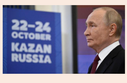
Glem at I intet aner om, hvordan man konfigurerer en firewall. Eller hvilken teknologi der giver jeres medarbejdere sikker adgang fra både lufthavn og hjemmekontor. Den slags *har* I ganske rigtigt folk eller partnere til at tage sig af.

Gør det, I er de bedste til: Vurdér de strategiske risici med skarp præcision, og brug så korte, effektive kommandoveje til at udstikke retningen for den taktiske indsats. Eller sagt med andre ord: Grib bolden og spil den klogt – jeres cybersikkerhedsfolk har brug for jer.

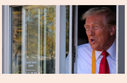
DEL GEM TIL SENERE

ANDRE LÆSER OGSÅ

Indsigt: Putin er stolt vært for topmøde – og gæsterne strømmer ind



14 dage til USA-valg: McDonald's kommenterer Trump-stunt



En kærlighedstragedie ødelagde hans liv to gange. Nu finder han mening i dansen

BØRSEN JOB

I SAMARBEJDE MED STEPSTONE

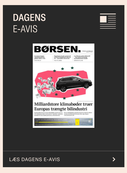
SE ALLE STILLINGER

Tech-investor: Et digitalt børskrak er ikke utænkeligt – sådan investerer jeg

Lyt med

Han var rådgiver for verdens største banker: Her ser han truslen mod dem

Lyt med



Lys fremtid for aktiemarkedet – Her kigger investorerne efter afkast

Lyt med

FORSIDEN LIGE NU

ØKONOMI LÆS SENERE

IMF: Væksten er for lav – det er tid til handling

AI

Nu lander Novos og Nvidias supercomputer: Hvad kan den?

UDLAND

Indsigt: Gæsterne strømmer ind til Putins topmøde

POLITIK

Her er de oplagte bud på SF's nye tronfølger