I en verden hvor cyberkriminalitet stiger i omfang og kompleksitet, er danske virksomheders ledelser og bestyrelser nødt til at forholde sig til risikoen for cyberangreb.

Jan 06, 2022 14:14 CET

Uansvarlig tilgang til cybersikkerhed ødelægger virksomheder

Debatindlæg bragt i Børsen, 4. januar 2022
Af CEO Jesper Zerlang, LogPoint

Mangel på cybersikkerhed er en af de mest kritiske trusler mod virksomheder i dag. Den sidste måned har budt på en lang række højtprofilerede angreb mod danske virksomheder, som illustrerer, hvor stor betydning angreb kan have for virksomheders forretning.

Salling Group er netop blevet ramt af et cyberangreb via en amerikansk it-

underleverandør, så mange HR-processer må udføres manuelt. Volvo blev for nogle dage siden ramt af et cyberangreb, hvor virksomhedens hemmelige data om forskning og produktudvikling blev stjålet. Derudover har angrebet givet driftsforstyrrelser på ubestemt tid, hvilket er en kostbar affære. I begyndelsen af december blev hotelkæden Nordic Choice ramt af et ransomwareangreb, der lagde alle 242 hotellers it-systemer ned og stadig til dels spænder ben for driften. Hotelkæden har i øvrigt måtte meddele deres gæster og medarbejdere om risikoen for lækkede persondata – ikke just betryggende.

Dramatiske konsekvenser

De tre nylige eksempler ovenfor illustrerer meget godt hvor alvorlige konsekvenser, cyberangreb kan føre med sig. Hæmmet produktivitet, direkte og indirekte finansielle tab på grund af løsesummer eller nedetid, læk af forretningskritisk information eller kunde- og medarbejderdata og skadet omdømme. Cyberangreb har kort sagt dramatiske konsekvenser for forretningen.

Desværre har mange har stadig for lang vej til at erkende, hvor altafgørende cybersikkerhed er.

Ifølge en ny rapport fra it-sikkerhedsvirksomheden Trendmicro er 93 pct. af danske topchefer villige til at ofre it-sikkerheden for bedre produktivitet, innovation eller kundeservice. Det er en helt skæv prioritering i forhold til det trusselsbillede, vi har i dag.

Innovation er ikke meget værd, hvis den bliver stjålet og lækket til konkurrenterne. Kundeservice er ikke meget værd, hvis medarbejderne ikke har adgang til systemerne. Og forbedringer i produktiviteten er ligegyldige, hvis driften bliver lagt ned i ugevis.

Faktisk er prioriteringen en decideret gambling med virksomhedens overlevelse.

Danske virksomheder er blandt de mest digitaliserede i verden, og det er af afgørende betydning, at topledelsen forstår alvoren af cybertruslen.

Truslen stiger, i takt med at virksomheder avancerer deres digitaliseringsrejse, implementerer flere forretningsapplikationer og flere medarbejdere arbejder hjemmefra. Samtidig med at angrebsfladen bliver større, finder de cyberkriminelle hele tiden på nye måder at udføre angreb på.

Det er umuligt at være foran de cyberkriminelle og dermed umuligt at holde dem helt ude af systemerne.

Virksomhedens immunsystem
Jeg plejer at sige, at niveauet af cybersikkerhed udgør virksomhedernes immunsystem.

Cybersikkerhed er så at sige den opbygning af teknologier, processer og menneskelig adfærd, der beskytter organisationen mod infektioner. Et godt immunforsvar kan ikke forhindre infektioner. Til gengæld kan det hurtigt slå dem ned. Et svækket immunforsvar derimod er både mere modtagelig over for infektioner, og konsekvenserne af infektion er ofte alvorlige.

Danske topchefer bør spørge sig selv, hvad de kan gøre for at styrke deres immunsystem optimalt.

I en verden, hvor cyberkriminalitet stiger i omfang og kompleksitet, er danske virksomheders ledelser og bestyrelser nødt til at forholde sig til risikoen for cyberangreb.

Cyberkriminalitet er blevet en uundgåelig risiko, som bør indgå i topledelsens strategiske overvejelser, ellers risikeres forretningen.

Derfor vil jeg opfordre danske topchefer landet over til personligt at tage ansvar ved dels at forstå de grundlæggende principper for god cyberhygiene samt strategisk og taktisk drøfte virksomhedens cyberberedskab med it-ledelsen, herunder at få beskrevet de konkrete planer for, hvad der skal ske, når de bliver angrebet. Det er simpelthen uansvarligt og manglende rettidig omhu at lade være.

Logpoint is a multinational, multicultural, and inclusive company. For more information, visit http://www.logpoint.com

Contacts

Maimouna Corr Fonsbøl
Press Contact
Head of PR
PR & Communications
mcf@logpoint.com
+45 25 66 82 98