PRESSEMEDDELELSE

PRESSEMEDDELELSE – Cybersikkerhed er dagligt til forhandling, men ansvaret ligger altid hos ledelsen

Pressemeddelelse · Rådgivning og teknik

Cybersikkerhed er mere end en teknisk disciplin, der kan parkeres hos it-afdelingen. Det rette setup kræver et organisatorisk og forretningskritisk blik, som virksomhedsledelsen skal tage ansvar for. Risikoanalyse er et godt sted for ledelsen at starte.

Aktuelle rapporter fra eksempelvis Erhvervsstyrelsen og Danmarks Statistik viser, at cybersikkerheden halter hos flere danske virksomheder – primært de små og mellemstore.

Som leder af Alexandra Instituttets afdeling for cybersikkerhed oplever jeg en stigende interesse for cybersikkerhed blandt danske virksomheder. Men samtidig er de i tvivl om, hvor aktiviteten skal placeres i organisationen, og hvilket niveau de skal vælge. For cybersikkerhed er langt mere end en teknisk disciplin. Den kræver et organisatorisk og forretningskritisk blik, som virksomhedsledelsen skal tage ansvar for. Risikoanalyse er et godt sted, ledelsen kan tage fat.

Ledelse, tag ansvar for virksomhedens cybersikkerhed!

De fleste tror stadig, at cybersikkerhed er en hardcore teknisk disciplin. Og ja, det er rigtigt nok. I sidste ende handler det om tekniske løsninger. Men cybersikkerhed handler i lige så høj grad om noget ikke-teknisk: Ansvar og prioritering. Derfor skal ansvaret for cybersikkerhed ikke parkeres i it-afdelingen eller uddelegeres, før man har haft de fornødne vurderinger internt og på ledelsesniveau.

Så mit klare råd til ledelsen lyder: Tag ansvar for virksomhedens cybersikkerhed. Det gælder de helt basale tiltag som firewall og opdateringer, men også de mere avancerede indsatser, i takt med at virksomheden digitaliserer sine løsninger og kobler produkter på nettet.

Jeg erkender, at cybersikkerhed i den grad handler om at finde det rette niveau. Ikke for meget og ikke for lidt. Og den beslutning skal ligge hos ledelsen, og en risikoanalyse kan være det grundlag, der kvalificerer beslutningen. En risikoanalyse kan være med til at afgøre, hvilke trusler der er mod virksomheden både teknisk og forretningsmæssigt. Derefter kan ledelsen vurdere: Skal vi outsource, skal vi opmande, eller skal vi trække eksperter ind ad hoc. Risikoanalyse er en måde at gøre cybersikkerhed nemmere tilgængeligt, mere overskueligt og systematiseret for de virksomheder, der ikke ved så meget om cybersikkerhed endnu.

Luk hullerne for hackerne

Man kan sammenligne cybersikkerhed med værn mod indtrængen af vand. Vil man gerne undgå indtrængen, vurderer man risikoen, man finder hullerne og man gør, hvad man kan for at lukke dem. For man ved, at dér hvor hullet er, søger vandet hen. Så det er der, man skal lægge sine kræfter.

Forestil dig, at du skal beskytte din virksomhed mod vand og derfor bygger et højt dige foran bygningen, mens baghaven står ubeskyttet. Eller dit dige er så højt hele vejen rundt, at du

mister både udsigt og kundebesøg, selvom vandet aldrig ville stå så højt. I skal vurdere risikoen for, om vandet vil løbe ind, hvor det vil løbe ind, samt hvilke tiltag I allerede gør i dag, og hvad I kunne gøre bedre. Måske skal I også inddrage eksperter undervejs.

Det samme gælder cybersikkerhed. En risikoanalyse hjælper med at forstå risikoen og er en måde, ledelse og medarbejdere kan komme hele vejen rundt om de forretningsmæssige og tekniske konsekvenser af ”hacker-huller” og dermed afdække behov for indsats og kompetencer.

Giv cybersikkerhed en central plads i virksomheden

Det kan være, at ledelsen har planer om at digitalisere nogle processer eller produkter for at bruge data på en ny måde og dermed skal kigge mod nye cybersikkerhedsteknologier? Ledelsen skal sørge for, at arbejdet med cybersikkerhed får plads på niveau med produktudvikling, forretningsudvikling, økonomi- og salgsafdeling. Cybersikkerhed handler om hele organisationens setup. Med andre ord: Cybersikkerhed er mange ting! Ikke kun firewall og passwords.

Jeg ser en tendens, hvor ledelsen vælger en boks, de mener kan sikre dem, og sætter de tjek ved den opgave. Men når vi spørger ind til, om de egentligt har brug for netop den boks, eller er det en anden boks, de skulle have haft, om leverandøren er ok, hvad med organisationen, og hvad er planen for digitalisering, så bliver de lidt tøvende. Det er de spørgsmål, ledelsen skal have på bordet, så de kan få svarene og dermed forstå behovet.

En risikoanalyse tager udgangspunkt i en valgt problemstilling. Og analysen behøver ikke være perfekt fra start. På den måde kommer man relativt let i gang med at få et sprog for trusselsniveau og for, hvordan man finder det rette cybersikkerhedsniveau. Et niveau der løbende skal diskuteres og vendes og ændres med en ledelse, der går forrest.

Cybersikkerhed handler om, hvilke data man har, hvilke man vil bruge, hvor digitaliseret man er. Ved man det, kan man udvikle sikre digitale løsninger, uanset om det er webløsninger eller IoT-produkter – dvs. klassiske produkter der kobles på nettet og dermed kan være mål for hackere.

Cybersikkerheden er til forhandling

Vores erfaringer viser, at når de forskellige fagfolk i virksomheden snakker sammen ud fra en model, som risikoanalysen bygger på, får de alle noget ud af det. Forretningsdelen

kommer med input til, hvilke ting der ikke må ske, fordi det gør for ondt på forretningen. Hvis f.eks. data lækkes, så dropper kunderne løsningen og finder en anden. Eller økonomi understreger, at man skal betale bøder, eller hvis man bliver hacket her, skal man bruge egne økonomiske ressourcer på at rydde op.

Pointen er, at cybersikkerhed er en kalkule. Mange tænker naturligt, at det sker jo ikke for os. Vores data er ligegyldige. Måske de tekniske siger: Jo det kunne ske for os. Eller udviklerne understreger, at det faktisk er koden, der kører på løsningen, der er forretningshemmelig, og derfor er det den, man skal sørge for at sikre.

Risikoanalyse handler egentligt om at blive enige om en skala. Det hele er lidt til forhandling. Hvad er konsekvensen? Det er det, analyserne skal tegne et billede af.

Dernæst kigger man på, hvad sandsynlighed er for, at det går galt. Måske har man allerede noget intern erfaring, der er vejledninger i ens branche om, hvor mange angreb der historisk har været på den type systemer og i verden udenfor. Det er også en god ide at holde øje med, hvilke trends der er. Læs generelle trusselsvurderinger. Og forvent ikke, at analysen er perfekt første gang. Det er den ikke. Så begynd i det små, men begynd nu!

Brug for mere info?

Ønsker du at vide, hvordan I kommer videre med en risikoanalyse, så find flere oplysninger om dine muligheder på vores hjemmeside: https://alexandra.dk/cybersikkerhed/

Læs rapporten: Samlede erfaringer fra 27 danske virksomheder: Sådan arbejder vi med sikre IoT-produkter på https://insights.alexandra.dk/acton/media/35392/cidi-rapport

Kontakt Gert Læssøe Mikkelsen, leder af Alexandra Instituttets afdeling for cybersikkerhed:

Mail: gert.l.mikkelsen@alexandra.dk obil: +45 24 26 99 11.

Kilde / Logo / Foto: Alexandra Instituttet

Online: https://pressemeddelelse.dk/pressemeddelelser/pressemeddelelse-cybersikkerhed-er-dagligt-til-forhandling-men-ansvaret-ligger-altid-hos-ledelsen/