Lappeløsninger giver falsk tryghed

by Mette Nielsen - tirsdag, marts 24, 2015

http://perspektiv.tdc.dk/lappeloesninger-giver-falsk-tryghed/

Lappeløsninger giver falsk tryghed

Med den fortsatte stigning i cyberkriminalitet i hele verden, er det tydeligt, at risikoen for angreb ikke vil forsvinde. Det er en risiko, alle virksomheder må leve med. Risikoens størrelse kan virksomheden dog selv være med til at bestemme. Læs her, hvordan sikkerhed mod angreb handler om risikovurdering og ikke kun investering i flere it-systemer.

Konsulenthuset PwCs seneste undersøgelse af informationssikkerheden anno 2015 viser, at antallet af cyberangreb globalt er steget fra 28,9 millioner angreb til 42,8 millioner på bare et år. I Europa alene er der sket en 41% stigning i angreb, hvilket gør Europa til højdespringeren i verden inden for cyberangreb. Det er et dystert udsyn, men ikke overraskende set i lyset af udbredelsen af mobility, social media, internet of things og andre supertrends. Cybertruslen følger den stigende udbredelse af teknologien og risikobilledet vokser i takt med brugen af ny teknologi.

Læs også: Du deler kontor med din største it-trussel

Risikovurdering er nøglen til sikkerhed

Det bliver sværere at købe sig til sikkerhed ved kun at investere i systemer. Det er også vigtigt at fokusere på informationer, data og processer, som er kritiske for forretningen. Samtidig spiller tiden og samfundsudviklingen ind, mener TDC.

”Vi har lige været igennem en årrække med økonomisk krise, hvor vi har oplevet, at danske virksomheder generelt er mere risikovillige i ønsket om at skabe et godt resultat. For at skabe overskud skærer man, hvor man kan og det er også gået ud over informationssikkerheden,” siger Lars Højberg, Teknisk sikkerhedschef hos TDC. Han forventer, at der i efter-krisetiden igen vil komme væsentligt mere fokus på informationssikkerhed, og her bør netop risikovurderinger bruges aktivt til at vurdere sikkerheden.

> IT-sikkerhed handler ikke kun om antivirus, firewalls og spamfiltre, men i høj grad også om prioritering af sikkerhedsindsatsen

”IT-sikkerhed handler ikke kun om antivirus, firewalls og spamfiltre, men i høj grad også om prioritering

af sikkerhedsindsatsen. Virksomheder må se på, hvilke informationer der er kritiske, og finde et passede sikkerhedsniveau. Det kræver, at man kortlægger sine aktiver og tager en beslutning om, hvor risikovillig man ønsker at være," siger Lars Højberg.

Læs også: Jeres it-sikkerhedsmur har allerede huller

Løb den lille risiko

En risikovurdering kan være et effektivt ledelsesredskab til at oversætte teknisk kompleksitet til potentielle økonomiske konsekvenser: Hvad betyder det for virksomhedens forretning, hvis kunderne ikke har adgang til virksomhedens hjemmeside? Eller hvis ordresystemer er blevet kompromitteret? Virksomheden får indsigt i, hvor i virksomheden man kan minimere investeringen i sikkerhed, når der ikke er tale om kritiske data. På denne måde prioriteres indsatsen.

Det drejer sig således om at kortlægge fire grundlæggende områder:

- Hvilket sikkerhedsniveau har vi i virksomheden i forhold til det aktuelle risikobillede for vores branche?
- Hvilket niveau vil vi gerne være på?
- Hvor stor er "kløften" mellem 1) og 2)?
- Prioritering af indsats

På baggrund af disse spørgsmål er det op til ledelsen at vurdere, om en øget indsats kan betale sig. En lille risiko kan være til at leve med, hvis man samtidig fokuserer sin indsats de rigtige steder i virksomheden. Dermed har man et klart billede af sin risikovillighed.

"Informationssikkerhed er en proces, man aldrig bliver færdig med. Trusselsbilledet ændrer sig hele tiden, så hvad, der var godt nok for et år siden, er ikke nødvendigvis godt nok længere," siger Lars Højbjerg, Teknisk sikkerhedschef hos TDC.

It-sikkerhed og VVS-arbejde

Indtil nu har mange virksomhedsledere set på it-sikkerhed som en teknisk specialiseret disciplin, på samme måde som de fleste kigger på VVS-arbejde.

Hvis et rør lækker, bestiller vi en blikkenslager til at lappe det utætte rør. Dermed er vi glade, lige indtil et andet rør lækker. Det svarer til, at man i virksomheden opdager en it-sikkerhedsbrist, og køber et system til at sikre det. Mange tænker, at hvis virksomheden bruger de rette it-sikkerhedsprodukter, vil der ikke være nogen "utætte rør" i virksomheden, Men hvad hjælper det at fokusere på utætheder, hvis hele rørføringen er dårlig?

"På den korte bane kan det virke billigere at være reaktiv og lappe de utætte rør, når skaden er sket. Men

lappeløsninger giver en falsk tryghed. I det lange løb kan det bedre betale sig at være proaktiv, så risikoen for et ødelæggende angreb minimeres. Det er umiddelbart forbundet med en større opgave, men ved at være proaktiv kan man undgå sikkerhedshændelser, der kan have en negativ effekt på bundlinjen," forklarer Lars Højberg.

Læs også: Den digitale verdens forpligtigelser

Link: PwCs undersøgelse af informationssikkerheden 2015