Cyberangreb - Hvad koster det?

4. juni 2018

Selvom frygten for cyberangreb er stigende, er det de færreste virksomheder, hvor ledelsen selv har et konkret overblik over risikoen og de mulige tab.

Ledelsen har en udfordring

Virksomhedens brug af internettet er kraftigt stigende, og internettet breder sig til stadig flere dele af virksomheden. Ledelsens udfordringer bliver ikke mindre af, at den bliver mødt af en stigende strøm af nyheder om cyberangreb og nye former for trusler. Nyheder, der forudsætter teknisk indsigt og kendskab til branchens seneste fagudtryk. I takt med tidsånden bruges der engelske forkortelser og fagudtryk.

Cyberangreb

Det klassiske angreb består i, at virksomhedens hjemmeside og e-mail-system modtager flere tusinde besøg samtidigt. Det store antal af besøg medfører, at virksomhedens hjemmesider, internetportaler og servere lukker ned.

Er virksomhedens forretningsdrift baseret på salg over nettet, er risikoen og tabet til at få øje på. Risikoen er dog typisk langt større i praksis. I dag er en meget stor del af virksomhedens kommunikation baseret på internettet, herunder e-mails. De fleste virksomheder har oplevet et kortere nedbrud i selskabets it-systemer, og forstiller man sig, at perioden forlænges til et par dage,

vil ledelsen ofte nå frem til, at tabet kan være betydeligt.

De fleste internetudbydere tilbyder i dag, at der kan tilkøbes beskyttelse mod cyberangreb, hvilket kan være med til at nedsætte risikoen.

Data i skyen

Den tekniske udvikling har medført, at virksomhedernes it-systemer og data i stigende omfang bliver sendt og kørt over internettet. Udliciteringen sker for at opnå stordriftsfordele, og derved billigere og mere effektiv drift af it-systemerne.

Selvom Cloud Hosting har sine fordele, medfører udliciteringen, at ledelsen skal forholde sig til, hvordan hosting leverandøren håndterer sikkerheden. I praksis kan det være svært at få et overblik over, hvordan leverandøren konkret håndterer risikoen. Hosting fjerner ikke risikoen, men flytter den.

IoT – Internet of Things

Det ser ud til, at internettet breder sig til alle dele af virksomhederne, og at vi kun lige er startet på denne udvikling. Det er ofte undervurderet, hvor mange enheder i virksomhederne der er koblet op på nettet. Det kan f.eks. være maskiner, systemer i produktionen, sensorer og alarmer.

Har virksomheden ikke et overblik over, hvilke enheder der er tilkoblet, har ledelsen ingen mulighed for at forholde sig til risikoen. Hertil kommer, at mange af enhederne, der er koblet op på nettet ude i virksomheden, har et relativt lavt sikkerhedsnivau.

Angreb i det skjulte

Hackernes jagt på penge bliver stadig mere kreativ og udspekuleret. Vi har set de første vellykkede angreb, hvor de kriminelle har skaffet sig oplysninger om, hvornår chefen er på ferie. Når økonomichefen herefter modtager en akut forespørgsel om pengeoverførsler, kan det være særdeles svært at opdage svindlen – før det er for sent.

Det er samtidig ved at være relativt almindeligt, at virksomhederne får hacket deres data, og først får adgang igen mod betaling. Løsesummen ligger typisk på et niveau, hvor det kan være svært ikke at tage imod tilbuddet.

Hvad koster det?

Når ledelsen skal vurdere risikoen og omkostningerne ved uautoriseret adgang og misbrug af virksomhedens data og it-systemer, kan opgaven være omfattende. Ud over de direkte tab kan virksomheden blive mødt med erstatningskrav og bøder. Hvad koster det? – For en del virksomheder vil de direkte tab kun udgøre en mindre del af tabet. Herudover kan virksomhederne blive mødt med erstatningskrav og bøder samt få betydelige imagetab.

Skrevet af:

Poul Erik Nielsen
Partner, statsaut. revisor
21 69 08 21 · pen@roesgaard.dk