CSIS Security Group

Corporate Security Check

Our passion - Your advantage

www.csis.dk

Vi kan bryde ind i din virksomhed!

Ingen ønsker at se sine fortrolige data blotlagt for offentlighedens kritiske blik, men alligevel sker det dagligt. Selv C20 virksomhederne har været udsat i pressen – med efterfølgende påtale. Årsagen er, at ressourcerne til IT-sikkerhed ofte prioriteres forkert i forhold til virksomhedens reelle trusselsbillede. Revisoren fortæller dig typisk, at du er teoretisk sikret, men er det tilstrækkeligt, hvis nogen alligevel kan snyde dine medarbejdere og systemer? Ved du, hvor nemt nogen kan få fat i dine data?
Næsten alle har en bagdør – ved du, hvor jeres er?

Fra kaos til konkret

Medierne er fulde af beretninger om virusangreb, forretningskritiske IT-systemer, der går i sort, identitetstyveri og mange andre uønskede hændelser. Det er ikke let at skelne mediestøj fra fakta. Kunsten er at identificere hvilke af truslerne, der er aktuelle for din virksomhed i relation til den kontekst, som virksomheden befinder sig i (branche, anvendte sikkerhedssystemer, konkurrenter m.m.).
Når alt kommer til alt, hvor godt er din virksomhed så rustet mod et målrettet hackerangreb?

IT-sikkerhed er generelt komplekst at forholde sig til. CSIS Security Group hjælper dig med at identificere, hvor du kan indsætte besparelser, og hvor ressourcerne og budgettet gør mest gavn. Således frigives ressourcer i virksomheden til mere værdiskabende formål.

Dit individuelle trusselsbillede

Hvad nytter det at sikre hoveddøren, hvis bagdøren står pivåben? Der findes en række love, regler og standarder, der tilsammen gør det uoverskueligt at vide, hvilke forpligtelser virksomheden skal leve op til. F.eks. i forbindelse med håndtering af fortrolige oplysninger, såsom kunde- og persondata. Kompleksiteten resulterer typisk i, at ressourcer og energi bliver udnyttet på en sådan måde, at væsentlige sikkerhedsforanstaltninger ofte overses.

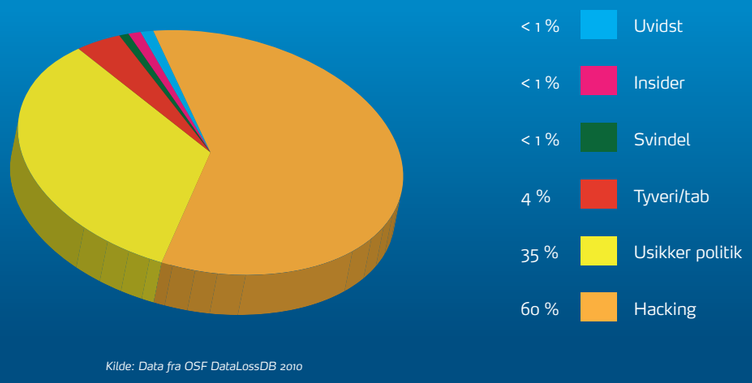
CSIS rådgiver virksomheder, så disse bliver i stand til at omprioritere deres ressourcer og rekonfigurere eksisterende IT-sikkerhedssystemer. Din virksomheds sikkerhedsniveau vil øges markant - uden ekstraomkostninger – samtidig med, at det reelle trusselsbillede imødekommes.

Medarbejderne som medspillere

IT-sikkerhed må ikke hindre produktiviteten – IT-sikkerhed skal sikre produktiviteten. Det skaber frustrerede medarbejdere, der anser IT-sikkerhed som en byrde, hvis dagligdagen besværliggøres for meget. Derfor handler et sikkerhedscheck også om at inddrage disse elementer. F.eks. nytter det ikke, at PDF dokumenter forbydes pga. IT-sikkerheden. I stedet kan en sikkerhedsprocedure indføres i det tidsrum, hvor klienterne ikke er sikkerhedsopdateret.

CSIS tror på, at medarbejdernes engagement er det vigtigste skridt på vejen til en bedre sikkerhed i virksomheden. Fokus er på learning-by-doing og seeing-is-believing ved at følge i hackerens fodspor. IT-sikkerhed er mere end et simpelt awareness-kursus. Medarbejderne skal inddrages ved en konkret demonstration af IT-indbrud i din virksomhed. Kun sådan samles medarbejderne, og bliver til medspillere i et fælles ønske om en optimal sikkerhed på arbejdspladsen.

Årsag til offentliggørelse af fortroligt materiale i 2009



Kilde: Data fra OSF DataLossDB 2010

Ved du om...

- **dine ressourcer til IT-sikkerhed er prioriteret korrekt?**
- **din virksomhed er beskyttet mod de relevante trusler?**
- **dine indkøb af IT-sikkerhedsudstyr overhovedet er nødvendigt?**
- **dine virksomhedsdata er eksponeret på nettet lige nu?**

CSIS Security Group A/S
Knabrostræde 3A
DK-1210 Copenhagen
VAT No. DK29523355

Phone: +45 88 13 60 30
Fax: +45 33 33 03 34
E-mail: ecrime@csis.dk

www.csis.dk