Aktuell Säkerhet

https://www.aktuellsakerhet.se/industrin-maste-utbilda-manniskor-i-vad-cyberattacker-innebar/

“Industrin måste utbilda människor i vad cyberattacker innebär”

2017-06-05

Vi lever i ett samhälle som är fullkomligt beroende av IT och data. Därför är också myndigheter, organisationer och företag beredda att betala stora pengar om någon skulle ta det ifrån dem.

– Ju mer beroende vi blir, desto större blir cyberhotet, säger Brian Lord, grundare av OBE.

Den europeiska cyberkonferensen NetEvents hålls i år i London, bara två dagar efter den senaste terrorattacken på London bridge och Borough market, då sju personer omkom och ett fyrtiotal skadades. Naturligt nog blir händelsen en slags avstamp för att lyfta de problem som världen i dag står inför.

– Det är ingen nyhet att terrororganisationer verkar online, dels för att koordinera sina attacker, men även för att sprida propaganda och att finansiera sina verksamheter, konstaterar Brian Lord.

Han förklarar vidare hur cybersäkerhet har blivit en större och mer aktuell fråga för stater och regeringar.

– Stater letar efter sätt att beväpna sig mot denna typ av verksamhet och därför tror jag att till exempel sociala medier kommer att se annorlunda ut om några år – regeringar måste samarbeta med sociala medie-företag för att hitta en gemensam lösning på hur plattformen för den enskilda staten ska se ut.

Ett växande fenomen är konceptet ransomware, som går ut på att hackare stjäl information – ofta från företag, organisationer och myndigheter – för att sedan kräva en lösensumma för att lämna tillbaka den.

– I dagens samhälle betalar organisationer vad som helst för att ha tillgång till data och detta utnyttjar förstås cyberbrottslingar.

Brian Lord pratar om att den som blir utsatt för en hackerattack förstås är ett offer – men även en typ av medbrottsling. Detta för att denne inte har gjort tillräckligt för säkra sin data.

– Det ligger ett värde i att stjäla data, både personlig data och organisationers. Därför inför EU nu GDPR, som även kommer att gälla i Storbritannien även om Brexit genomförs. Genom GDPR kommer företag kunna bötfällas om de inte håller personlig data säker.

Slutligen berör han spionage stater emellan och det kanske senaste och mest berömda caset, med trolig rysk inblandning i det amerikanska presidentvalet 2016.

– Vi ska inte låta oss luras – det är inte bara Ryssland som spionerar på andra stater. Detta är något de flesta stater sysslar med. Fenomen som falska nyheter och statligt spionage har funnits länge, problemet är bara att vi inte har kunnat identifiera det. Detta måste förändras.

– Det handlar om att jobba på alla nivåer, från stat till regering, media, industrin till enskilda personer för att tillsammans motverka cyberhotet. Genom att samarbeta och utbilda människor kan vi få de verktyg som behövs för att skydda oss mot denna typ av brottslighet, avslutar han.