LOGPOINT

Undervurderer virksomheder nødvendigheden af it-sikkerhed, kan de ende som ufrivillig aktør i den voksende cyberkrig

May 16, 2022 11:02 CEST

Du kan ende som ufrivillig aktør i cyberkrigen

Undervurderer virksomheder nødvendigheden af it-sikkerhed, kan de ende som ufrivillig aktør i den voksende cyberkrig

Jesper Zerlang, adm. direktør, Logpoint

“Mange virksomheder ser ikke sig selv som mål for it-kriminelle og tager derfor ikke de nødvendige forholdsregler,” står der i regeringens udspil til en digitaliseringsstrategi for Danmark, som blev præsenteret for nyligt. Mange ledere har stadig svært ved at forestille sig at netop deres virksomhed skulle

blive målet for et cyberangreb. Men de tager grueligt fejl, og krigen i Ukraine har understreget risikoen ved at undervurdere opgaven med at sikre sig mod angreb i cyberspace.

I cyberspace er vi nemlig alle potentielt en del af krigen. Rusland er i fuld gang med at forberede og udføre angreb på den vestlige verden. Angreb, som kan skade virksomheder og økonomier, ryste vores tillid til offentlige myndigheder, forstyrre kommunikationen og vores frie, uafhængige medier. Derfor har alle virksomheder og organisationer en forpligtelse til at sørge for stærkt cyberforsvar og forberede sig på en situation, hvor truslen fra Rusland antager hidtil usete dimensioner. For der er mange scenarier, som kan gøre en til et gidsel eller en ufrivillig aktør i en global cyberkrig.

En af de statsstøttede hackeres yndlingsmetoder er at angribe virksomhedernes forsyningskæder, de såkaldte supply chain-angreb, hvor angriberne får adgang til virksomhedens systemer gennem en tæt partner eller underleverandør, der ikke har styr på egen cybersikkerhed. Eksempelvis var bilfabrikanten Toyota for nylig tvunget til at lukke 14 fabrikker og 28 produktionslinjer en hel dag på grund af et angreb, som ramte virksomheden gennem en underleverandør.

Det er nu du skal handle

En anden udbredt metode er de såkaldte ddos-angreb, som lammer digitale systemer ved at overbelaste servere og infrastruktur, hvilket vi har set flere eksempler på under Ukraine-krigen. Angriberne overtager kontrollen med ubeskyttede enheder på nettet og bruger dem som et værktøj til at generere store trafikmængder, der kan lamme vitale dele af vores infrastruktur. Forestil dig at russiske hackere tager kontrol med dine systemer og bruger dem som et springbræt til at angribe dine egne samarbejdspartnere eller kunder.

Ransomware-angreb har trukket store overskrifter de seneste år med angreb på store virksomheder som Maersk, ISS, William Demant og Vestas. Mange virksomheder vælger at klare sig gennem angrebet ved at lukke deres systemer og forretninger i dage eller uger – andre vælger at betale. I USA betalte forsikringsselskabet CNA sidste år over 200 mio. kroner for at genetablere adgangen sine systemer. Men i en cyberkrig risikerer man, at ransomware-angrebene i højere grad bliver destruktive, og at data slet ikke kan genskabes.

Der er flere ransomware-grupper, som støtter Rusland, eller som opererer i sikkerhed fra Rusland. Hvis man ender i kløerne på en af disse grupper, så risikerer man at miste adgangen til sine data for altid, eller man betaler en løsesum, som kan være med til at finansiere hybridkrigen. Cyberansvarlighed har altid været samfundssind og social ansvarlighed, men det har aldrig før været så klart, hvor vigtigt det er at leve op til sine forpligtelser og sikre, at man ikke ender som en ufrivillig aktør i den globale cyberkrig.

Det er nu, du skal handle, hvis du ikke allerede har sat cybersikkerhed på toppen af virksomhedens agenda, som en integreret del af forretningsstrategien og rent operationelt i din organisation. Der er behov for et opgør med det udbredte dogme, at cyberangreb rammer ikke os. Det kræver kun en enkelt sprække i forsvarsværket, en enkelt cyberkriminel eller en uforsigtig eller utilfreds medarbejder, før der er adgang til virksomhedens systemer, og man bliver trukket ind i cyberkrigen.

Ufrivillig aktør

Der er en global talentkrise inden for cybersikkerhed, hvor der mangler millioner af kvalificerede medarbejdere. Derfor er det oplagt at vende blikket mod automatiserede løsninger baseret på kunstig intelligens eller samarbejde med servicevirksomheder, der har kompetencer til at opdage og bekæmpe cybertrusler 24/7.

Krigen i Ukraine har fået vestlige virksomheder og organisationer til at stå i kø for at erklære deres støtte til Ukraine, og mange virksomheder er stoppet med at lave forretning i Rusland – enten på grund af officielle sanktioner, for at sikre sit gode ry eller for at leve op til egne csr-standarder.

Hvis man overser eller ignorerer det faktum, at cybersikkerhed også er en csr-forpligtelse, så kommer virksomheder, kunderne, samarbejdspartnere og medarbejdere i farezonen, og man risikerer at blive en ufrivillig aktør og støtte for Rusland i landets cyberkrig.

Oprindeligt bragt som kronik i dagbladet Børsen, 16. maj 2022

About Logpoint

Logpoint is the creator of a reliable, innovative cybersecurity operations platform — empowering organizations worldwide to thrive in a world of evolving threats. By combining sophisticated technology and a profound understanding of customer challenges, LogPoint bolsters security teams' capabilities while helping them combat current and future threats. Logpoint offers SIEM, UEBA, SOAR and BCS technologies converged into a complete platform that efficiently detects threats, minimizes false positives, autonomously prioritizes risks, responds to incidents, and much more. Headquartered in Copenhagen, Denmark, with offices around the world, Logpoint is a multinational, multicultural, and inclusive company. For more information, visit http://www.logpoint.com

Contacts

Maimouna Corr Fonsbøl
Press Contact
Head of PR
PR & Communications
mcf@logpoint.com
+45 25 66 82 98