NetDesign

5G, Artificial intelligence, Machine Learning og Internet of Things åbner for mange nye muligheder. Samtidig stiger kompleksiteten i det digitale trusselsbillede - og virksomhederne bliver mere sårbare på flere områder.

Vi har talt med to af vores sikkerheds-eksperter om, hvordan du får ro i sindet, når de nye teknologier rykker ind.

Fra frygt til fokus: Gør jeres it-sikkerhed klar til nye teknologier

Digitaliseringen har fart på

Det kommende 5G-netværk åbner for et nyt spor på den digitale motorvej, hvor hastigheden er mangedoblet og mulighederne holder i kø for at blive udnyttet. Uanset størrelsen på din virksomhed, så vil ny teknologi i de kommende år give nye forretningsmuligheder, som vi tidligere kun kunne forestille os.

> *5G og IoT ændrer måden vi agerer på. Flere sammenkoblede enheder og systemer giver en større angrebsflade og flere punkter, hvor du kan være sårbar. Du kan ikke bare installere en firewall i dit IoT-miljø, så du må begrænse risikoen på andre måder. Der er ingen grund til panik, men brug sund fornuft.*

Thomas Bo Birch
Product Manager, Cyber Security, NetDesign

For eksempel via Internet of Things (IoT), hvor forbundne enheder kan bruge kræfterne fra 5G til at kommunikere lynhurtigt og præcist til blandt andet at styre temperaturer, overvåge processer eller angive når en maskindel trænger til service.

Frygt for fremtiden

Hos de ansvarlige for it-sikkerheden kan glæden over de mange muligheder dog let blive overskygget af bekymring over, hvordan de nye enheder påvirker virksomhedens samlede it-sikkerhed.

For kreative cyber-kriminelle er konstant på jagt efter nye metoder og kunne for eksempel finde på at udnytte sårbare IoT-enheder til at få adgang eller udnytte båndbredden i 5G til at give et DDoS-angreb flere muskler.

IoT med eget netværk

Det er blandt andet vigtigt at være bevidst om, hvilke data du vil beskytte, for eksempel kundedata, ordresystem og e-mail. Tommelfingerreglen er, at jo vigtigere noget er for din virksomhed, jo bedre skal det være beskyttet. For eksempel ved at holde dine IoT-enheder isoleret fra resten af netværket.

> *Ligesom de fleste virksomheder har et separat gæstenetværk, så bør de også have et dedikeret net til IoT-komponenter som er adskilt fra det administrative netværk.*

Thomas Bo Birch
Product Manager, Cyber Security, NetDesign

Få fod på det basale

En anden sikkerhedsekspert, Tommy Abrahamsson fra sikkerhedsvirksomheden SECU, der for nylig blev købt af TDC Erhverv og NetDesign, peger ligeledes på sund fornuft og faste rutiner som modgift til sikkerhedsbekymringer.

> Mange virksomheder kæmper stadig med basale ting som at få scannet for sårbarheder og patchet regelmæssigt. Hvis der kommer styr på det grundlæggende, vil virksomheden også være mere robust overfor trusler fra nye teknologier.

Tommy Abrahamsson
Sikkerhedsekspert, SECU

Få "Peace of Mind" med NetDesign

Scan for sårbarheder hver måned

I mange virksomheder kommer it-sikkerheden let til at drukne mellem de daglige opgaver. Her kan det være værd at overveje at outsource dele af it-driften via en Managed Service-aftale. Men i bund og grund handler det om at oparbejde gode vaner, både hos de it-ansvarlige og de øvrige medarbejdere.

> *"It-sikkerhed skal ikke være noget, du har på dagsordenen et par gange om året. Scan løbende for sårbarheder, mindst en gang om måneden, og sæt tid og ressourcer af til at fikse de fejl, du finder. Det er især vigtigt med regelmæssige interne sårbarhedsscanninger, samt en rutine til at patche, for det er typisk her, du virkelig kan få en sikkerhedsgevinst.*

Tommy Abrahamsson
Sikkerhedsekspert, SECU

Brug ny teknologi til at styrke sikkerheden

Heldigvis findes der mange gode værktøjer, der gør det lettere at få sikkerhedsrutinerne på plads. Du kan for eksempel købe en plug-and-play sårbarhedsscanner med opdaterede signaturer, der trawler dit netværk igennem for usikre applikationer og manglende opdateringer.

Et værn mod ny og ukendt malware kan være antivirus med machine learning, der kan genkende typiske adfærdsmønstre i ondsindet software og på den måde identificere en trussel uden at kende den i forvejen.

Password-sikkerheden kan også styrkes med et virtuelt password-pengeskab. Her opbevares alle virksomhedens passwords, og pengeskabet kan indstilles til automatisk at udskifte dem løbende. Herefter skal medarbejderne blot holde styr på deres login til pengeskabet, hvilket kan sikres med to-faktor validering. Det sikrer blandt andet, at medarbejdere, der forlader virksomheden, ikke længere har adgang til de forskellige passwords.

Få "Peace of Mind" med NetDesign

I NetDesign vil vi gerne sikre dig "Peace of Mind " i netværksløsningerne. Det betyder, at du fremover, blandt andet via vores Managed Services, i endnu højere grad, kan få fleksible netværksløsninger med indbygget sikkerhed, overvåget og serviceret 24/7.

Læs mere om vores sikkerhedsløsninger her

Læs mere:
netdesign.dk

Følg os på:
LinkedIn

Ring til os:
+45 4435 8000

Skriv til os:
kundecenteret@netdesign.dk

NetDesign, København, CVR 40 07 52 91 Communication/MC 2048.1921