360 Graders Proaktiv Cyber Security

4 udfordringer og løsningen som 80% vælger

ADDPRO

Hvor kan hackeren komme ind hos jer?

Står jeres døre pivåbne for hackerangreb?

Er I et let bytte for hackeren?

Modern workplace giver frihed til at arbejde fleksibelt og hvor som helst. Men hackeren får også større frihed – til at kigge indenfor hos jer, stjæle data, afpresse og lave en masse ravage, som koster kassen!

De senere års stigende hjemmearbejde – og arbejde overalt på forskellige enheder – har været en øjenåbner for mange virksomheder, der har indset, at IT-sikkerhed er andet og langt mere end en firewall og et antivirus program. Og det er ikke kun de store virksomheder, der rammes! Også små og mellemstore virksomheder er en lækkerbisken for hackeren. Især hvis dørene står pivåbne og signalerer "kom bare ind..."

Hvordan ser det ud hos jer?

1

Er det måske for nemt at logge på?

Det er ikke nogen svær opgave for en dreven hacker at skaffe sig et brugernavn og en adgangskode. Så hvis det er det eneste, der kræves for at logge på hos jer, så står døren nærmest helt åben. Men I kan gøre det svært for hackeren...

Med multifaktor godkendelse indfører I adgangskontrol til jeres Microsoft 365. Det er et ekstra sikkerhedslag på toppen af installationen, der sikrer, at fremmede ikke får adgang til mails og virksomhedens data generelt. Identitetssvindel som eksempelvis CEO Fraud minimeres. Multifaktor godkendelse vinder større og større udbredelse i kampen mod cyberangreb.

Microsoft Azure Multi-Factor Authentication er en del af AddPros proaktive sikkerhedssystem Security-aaS

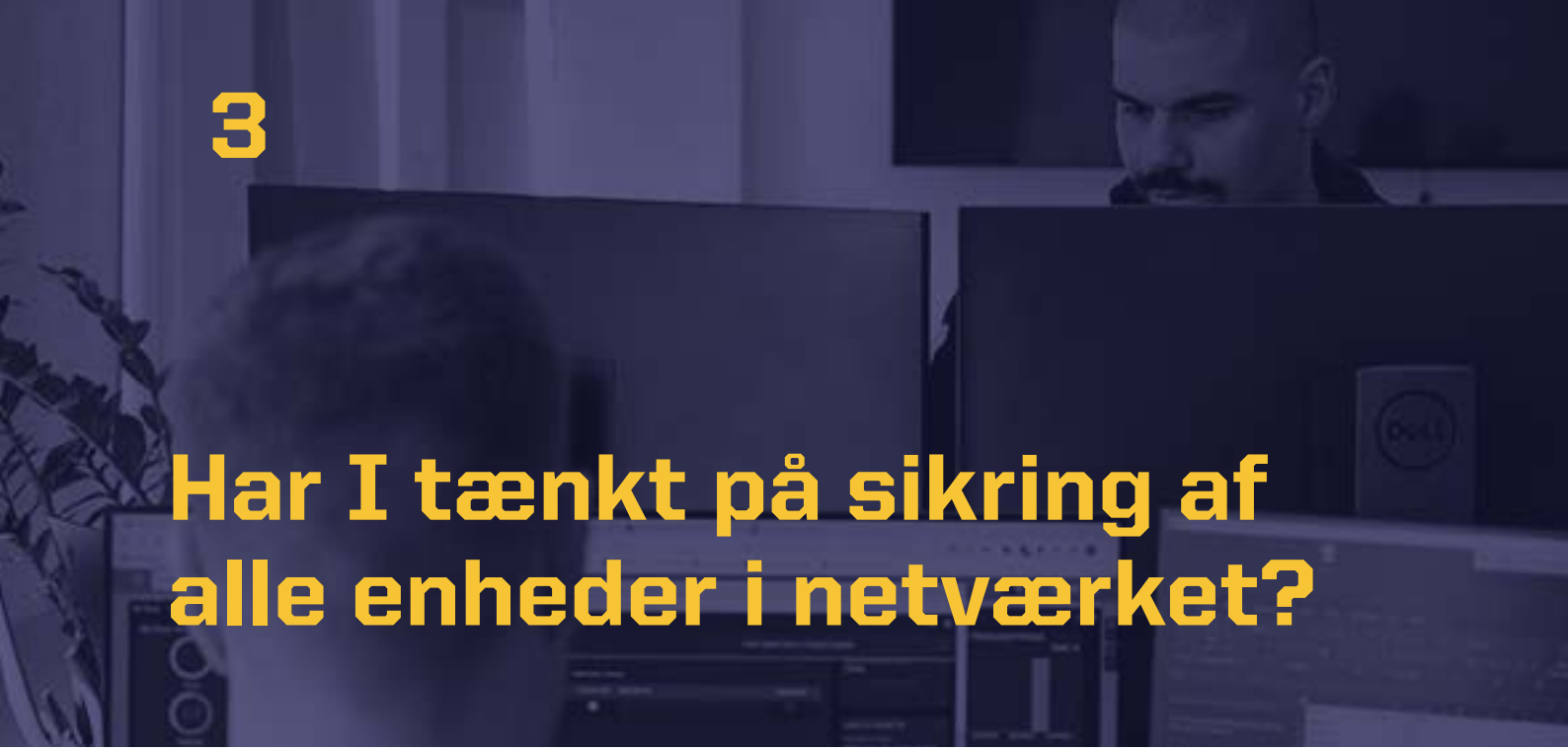
2

Har I uopdateret software, der lokker hackeren til?

Noget af det, der kan skærpe en hackers appetit på at snige sig indenfor, er uopdateret software. Faktisk har vi her en af de helt store årsager til cyberangreb. Har I en procedure for opdatering?

Ellers vil vi gerne spille Remote Monitoring & Management på banen. Med dette værktøj styres opdateringer fra centralt hold, så alle enheder altid er helt opdateret. Skulle en bruger have slået opdatering fra, kan de presses igennem. Flere og flere virksomheder vælger central styring af opdateringer, netop fordi det en lavthængende frugt, man nemt kan plukke i kampen mod indtrængerne.

Remote Monitoring & Management (RMM) indgår i AddPros proaktive sikkerhedssystem Security-aaS



3

Har I tænkt på sikring af alle enheder i netværket?

Hackeren kan godt lide intern datatrafik, for han ved, at den kan åbne mange veje ind i virksomheden. Eksempelvis synes han, IoT er interessant, for han kan jo lige så godt skaffe sig adgang via et kamera eller andet udstyr som en PC.

Her vil vi gerne fortælle dig om Unified Threat Management. Med UTM scannes al trafik mellem interne enheder på jeres lokale netværk samt al trafik, som rammer centrale punkter i servernetværket for datacenter/cloud. Løsningen inkluderer også global scanning for kommende trusler.

Behovet skyldes, at cyberangreb nu er mere baseret på sårbarheder på tværs af virksomheden. Især målrettet IoT enheder som for eksempel et kamera eller netværksudstyr såsom printere, access points, enheder med mere. Med løsningen kan I beskytte jer mod det værst tænkelige angreb, som kan lamme hele IT infrastrukturen eller resultere i et totalt nedbrud.

I kan få Unified Threat Management med i AddPros proaktive sikkerhedssystem Security-aaS

4

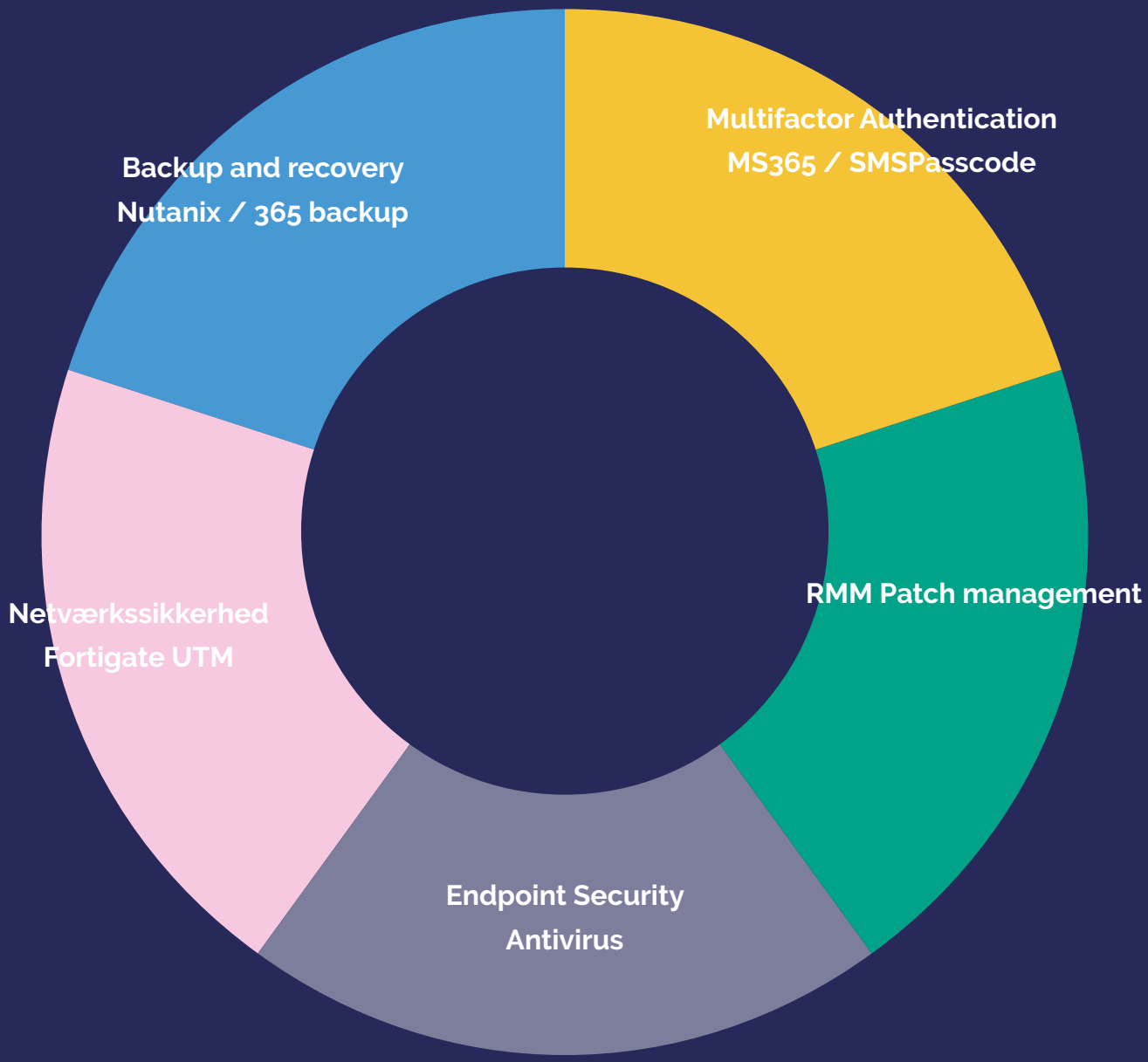
Får jeres antivirusprogram smilet frem?

Helt ærligt – mange hackere er ret smarte, og når de støder på en spinkel forhindring, kan man forestille sig, at de trækker lidt på smilebåndet. Er jeres antivirus sådan lidt grinagtigt svagt og outdatet? Lever det op til at være den primære beskyttelse, når dine brugere færdes på internettet?

Hvis du mener, der er en udfordring her, så kan vi tilbyde dig et antivirusprogram, der vil noget. Det kan godt være, du har fået et forærende som en del af en samlet programpakke. Men vi foretrækker en løsning fra en producent, der har antivirus som primær fokus.

Antivirus er en del af AddPros proaktive sikkerhedssystem Security-aaS

Proaktiv 360 graders Cyber Security



Vigtigste punkter i en samlet sikkerhedsløsning

Lad os hjælpe med at finde og lukke hullerne inden det er for sent!

IT-sikkerhed er en strategisk disciplin, der involverer hele virksomheden, og som skal tage højde for både indefra- og udefrakommende udfordringer for virksomhedens IT-sikkerhed.

Derfor vil vi gerne i dialog med dig og udarbejde en Gap&fit-analyse, som fortæller præcist hvor I står, og hvad der skal gøres.

Med en Gap&fit-analyse skaber du sikkerhed for, at din virksomhed efterlever standarden i forhold til jeres særlige profil, og du bringer virksomheden op på et sikkerhedsniveau, der både matcher trusselsbilledet og virksomhedens risikoprofil.

Vil du vide mere?

Kontakt os på:
Tlf.: +45 3133 4455
E-mail: info@addpro.dk

Læs mere om AddPro Danmark på addpro.dk

ADDPRO