10 gode råd der sikrer jer mod cyberangreb i Office 365

1 Aktiver logging

Vi anbefaler, at I aktiverer logning på fx postkasse-audit. I tilfælde af angreb fra cyberkriminelle er det meget begrænset, hvad man kan se bagefter. Man kan skræddersy, hvad der skal logges, men som minimum bør default-logging vælges. Audit logs gemmes i 90 dage og koster ikke en ekstra licens.

2 Håndter jeres legacy-protokoller

I Office 365 er følgende protokoller slået til pr. default: SMTP, POP3, IMAP, Exchange Web Services (EWS) og Exchange ActiveSync. Cyberkriminelle benytter ovenstående protokoller til blandt andet at lave password spray-angreb. Udfordringen med disse protokoller er, at de er så gamle, at de ikke understøtter multi-factor authentication (MFA).

Microsoft anbefaler, at man slår alle legacy-protokoller fra. Dette kræver dog, at man lige undersøger, om der er services, der fx benytter SMTP eller IMAP til noget.

Netop IMAP kan være problematisk, da dette er den eneste måde, man kan få adgang til delte postkasser via sin mobiltelefon på.

SMTP bruges oftest til mail relay og det kan være, at løsninger, der benytter sig af den type konfiguration, skal laves om. Bemærk, at der for at kunne slå nogle protokoller fra, kræves et nyere OS på mobilen.

3 Gør multi-faktor autentificering mulig

Multi-faktor autentificering MFA, er en ekstra sikkerhed, så der ud over brugernavn og password kræves en ekstra faktor, fx en pinkode. Det kan laves uden ekstra licens. Vi anbefaler, at alle brugere benytter MFA, hvor dette er muligt.

4 Sæt regler om betinget adgang

Med betinget adgang, conditional access, kan man lave smarte regler, så I ikke så ofte skal autentificere med MFA. Hvis brugeren logger ind fra et andet land, registreres dette ved hjælp af funktionen “umulig rejse”, og brugeren får en meddelelse om at skulle foretage et login med MFA.

En umulig rejse er fx, at brugeren logger ind et sted i Danmark via en dansk ip-adresse og kort tid efter logger ind i et andet land, hvor brugeren umuligt kunne nå at rejse til på den tid, der er gået. Dette kan godt være en falsk positiv. I sådanne tilfælde vil brugeren blive mødt af et ekstra MFA-login.

Betinget adgang handler ikke kun om Office 365 men om alle applikationer, man har i Microsoft Azure. Conditional access kræver en ekstra licens.

5 Brug portalen Microsoft Office 365 Secure Score

365 Secure Score er en portal, hvor Office 365-administratorer kan gå ind og se, hvordan de ligger sammenlignet med andre virksomheder.

Det er ikke meningen, at man skal gå efter at få topscore i sit Secure Score. Man skal have et så højt tal som muligt, som passer til den virksomhed, man arbejder for. Nogle forslag til forbedringer koster ekstra licenser, så det skal man også være opmærksom på.

6 Få den rigtige licens

Vi oplever tit, at mange ikke har den licens de ønsker sig, når først det er gået galt.

Man kan komme langt med de billigste licenser, fx MFA og audit logging. Men fx anti-phishing, safe links og safe attachments er kun tilgængelige med bestemte typer licenser. Ligeledes er der en del af sikkerhedsløsningerne i portalen, som kræver en ekstra licens.

Vi anbefaler, at I kigger på at tilkøbe ekstra Office 365-sikkerhedsprodukter. Hvis I kan stoppe en sikkerhedshændelse inden den starter, kan I spare jer en masse tid, penge og bekymringer.

PwC oplever, at det øger muligheden for at opklare hændelsen, hvis man har licenser, der giver adgang til sikkerhedsprodukterne. I skrivende stund hedder de:
Office 365 Enterprise E3/E5- og Azure AD P1/P2-licens.

7 Evaluer jeres backup-løsning

Evaluer, om den backup-løsning Microsoft leverer er tilstrækkelig. Der findes mange andre leverandører, der kan hjælpe med at lave backup af Office 365, OneDrive, Sharepoint osv.

8 Indfør SPF-, DKIM- og DMARC-sikkerhedstiltag

Disse sikkerhedstiltag hjælper modtageren med at sikre sig mod e-mail-spoofing. Vi anbefaler, at I indfører disse tiltag, da e-mail-spoofing bliver mere kompliceret at udføre.

Sender Policy Framework (SPF)
Sender Policy Framework (SPF) er en e-mailvalideringsstandard, designet til at stoppe e-mail-spoofing. SPF giver virksomheden mulighed for at specificere hvilke mailservere, der må sende e-mails fra virksomhedens domain.

DomainKeys Identified Mail (DKIM)
DKIM er kort fortalt en metode, hvor e-mails mellem en afsender og en modtager bliver verificeret som kommende fra den rigtige kilde. DKIM benytter en digital signatur, der tilføjes e-mailens header af den afsendende mailserver.Der laves en DNS record i virksomhedens eksterne DNS-server, som indeholder den offentlige nøgle for den digitale signatur, som e-mail-headeren bliver signet med.

Domain Message Authentication Reporting & Conformance (DMARC)
DMARC kigger efter, om afsenderen benytter ovenstående, eller bare en af delene, og ud fra det vurderes det, hvad der skal gøres, hvis e-mailen ikke kan verificeres.

Hvis e-mailen ikke kan verificeres gennem ovenstående, kigger mailsystemet på DMARC-manualen og afgør derfra, om mailen skal i karantæne, eller om den skal fjernes helt.

9 Træn opmærksomheden

PwC anbefaler, at I træner medarbejderne i at være opmærksomme på tvivlsomme e-mails. Det kan eventuelt være links, der skal trykkes på, fakturaer, der skal betales, og sider, der spørger efter brugernavn og password.

Ligeledes skal dine medarbejderne instrueres i ikke at godkende MFA-godkendelse, med mindre de selv har bedt om det.

10 Procedurer

Vi anbefaler, at I laver klare aftaler omkring fakturering. E-mails, som er videresendt fra chefen, skal fx altid følges op af et telefonopkald.

Fakturaer, der ikke ser helt rigtige ud, skal man altid lave en ekstra kontrol på. Der kan fx være tale om forkert angivelse af moms, at fakturaen ser mærkelig ud, eller at den har forkert ordlyd (Google Translate).

Lav helt klare regler og procedurer i fx sommerferien. PwC ser ofte denne periode udnyttet, når den, der normalt sidder med betalingen af fakturaer, har ferie.

Kontakt

Mads Nørgaard Madsen
Partner
M. + 45 2811 1592
E. mads.norgaard.madsen@pwc.com

Thomas Grandjean
Director
M. + 45 2811 1792
E. thomas.grandjean@pwc.com