M365 sikkerhetsvarsler

AUTOMATISK & PROAKTIV

Sørg for at IT-teamet får sikkerhetsvarsler

M365-varsler

Din bedrift er helt avhengig av M365 for daglig drift. Hva ville skje dersom du mistet tilgang til epost, filer, SharePoint, eller Teams på grunn av manglende sikkerhetstiltak? Det er på tide å ta Microsoft-sikkerhet på alvor og bli proaktiv med ditt cyber-forsvar.

Microsoft 365 utfører omfattende logging over aktiviteter. De fleste organisasjoner har millioner av oppføringer i loggene *hver måned* - data som viser mønster i brukeratferd. Hvordan kan man bruke denne informasjonen til å forhindre datainnbrudd? Jo, vi kan lage en sikkerhets-policy med varsler basert på *utypisk* brukeratferd i din organisasjon. Vi kan presisere bl.a. hyppighet, risikonivå, og kategori på hvert varsel (142 mulige varsler) for å sikre at alvorlige hendelser blir håndtert med en gang.

7 eksempler på mistenkelige aktiviteter som vil utløse et varsel

- **Innlogging fra mistenkelig sted**
- **Utvidelse av administratorrettigheter for Exchange**
- **Endring i applikasjoner** (forhindre nedetid eller feilkonfigurering av M365-verktøy)
- **Epost-videresending** (forhindre overvåking av epost-innhold av uvedkommende)
- **Mislykkede påloggingsforsøk** (forhindre "brute-force" taktikker)
- **Nedlasting av store mengder data**
- **Sletting av uvanlig store mengder data**

Hvorfor M365-varsler?

- IT-teamet blir varslet umiddelbart om mistenkelig brukeratferd.
- IT-teamet får muligheten til å stoppe mistenkelig aktivitet umiddelbart.
- Varsler blir rangert slik at IT-teamet kan reagere raskt på de mest alvorlige hendelsene.
- Det beste og billigste cyberforsvaret er proaktivt. *Ikke vent til det er for sent.*

Hvordan kan vi hjelpe?

Oppgrader din MS-sikkerhetsstrategi fra reaktiv til *proaktiv* med vår avanserte sikkerhetstjeneste.

M365-varsler

Få kontinuerlig overvåking med varsler om brukeradferd, regler, eller innstillinger som svekker sikkerheten i din virksomhet.