WhitePaper

E-mail sikkerhed
10 enkelte råd til bedre sikkerhed

SAC·IT
INSTANT TECHNOLOGY

Indhold

Størstedelen af alle cyberangreb og datalækager involverer e-mail, hvilket gør det til den største trussel mod virksomhedens it-sikkerhed.

01. Skift til multifaktorgodkendelse (MFA)

Den traditionelle brugernavn-adgangskode-logon er ikke længere stærk nok til at sikre e-mail-konti. Brugernavn og adgangskode kan mistes eller stjæles, hvorfor multi-faktor autentificering tilføjer et afgørende sikkerhedslag under login og minimerer risikoen for stjålne legitimationsoplysninger. **Multifaktorgodkendelse** er den nemmeste og mest effektive måde at opgradere sikkerheden i din virksomhed.

> **Ifølge Microsoft kan MFA blokere over 99,9 procent af angreb, der har som formål at kompromittere dine konti. Aktivering af MFA er en af de nemmeste ting, du kan gøre for at beskytte dine e-mail-konti og et absolut minimum for at forhindre adgang for hackere.**

Multifaktorgodkendelse kaldes også to-trins-godkendelse og som navnet viser, kræves der to trin for at få adgang. Trin to kan f.eks. være en sms-kode på telefonen og dette ekstra trin forhindrer hackere i at få adgang, hvis de har opsnappet din adgangskode. Dog er sms-koder også mulige for hackere at opfange. Den nyeste og mere sikre metode er en godkender-app på mobiltelefonen, som kendt fra offentlige instanser og banker, hvor du blot skal trykke "godkend" i stedet for manuelt at indtaste en kode.

Enkeltpersoner kan nemt opsætte multifaktorgodkendelse til konti, f.eks. Google og Microsoft konti.

Virksomheder, der bruger Microsoft 365, kan tilføje en indstilling der kræver, at brugere næste gang logger ind med **multifaktorgodkendelse** for at få adgang.

Nogle kan synes, at MFA er besværligt, men det andet trin i godkendelsen udføres generelt kun den første gang, der logges på en enhed, samt når adgangskoden er blevet skiftet. Dette er tilstrækkeligt til at forhindre angreb, da uautoriserede vil blive stoppet ved trin to.

02. Bloker ældre godkendelse

I Azure Cloud-tjenester bruges fortsat ældre brugergodkendelsesprotokoller, som inkluderer SMTP, IMAP, POP og MAPI.

Disse ældre autentificeringsteknikker understøtter ikke moderne sikkerhedsprotokoller som f.eks. multifaktorgodkendelse, hvilket gør dem til nemme adgangsveje for hackere. Disse forældede sikkerhedsprotokoller bør udskiftes med nye og mere sikre adgangsveje.

Microsoft annoncerede for nylig planer om at deaktivere nogle grundlæggende godkendelsesmetoder i Exchange Online. Dette for at lave mere sikre e-mail-konti til alle brugere.

> **"Blokering af enheder som ikke kan bruge MFA er en effektiv løsning, for at undgå hackeres adgangsmulighed."**

Det er desuden muligt at blokere for 3. parts applikationers adgang til virksomhedens data og kun gøre dette muligt med Microsoft O365 applikationer som kan kontrolleres centralt i Intune.

03. Aktiver Unified Audit Log (UAL)

Har du i organisationen et incident, har du med aktiveret Unified Audit log fuld tradability, og kan derfor spore alle de handlinger der er foretaget på systemet, og dermed kan du lettere finde problemet når og hvis der alligevel skulle være et angreb udefra.

Unified Audit Log registrerer forskellige hændelser fra Exchange Online, Azure Directory, Teams og andre Office 365-tjenester. Loggen giver dig et overblik over tidligere og igangværende aktiviteter i Azure-miljøet.

UAL giver også mulighed for at fortryde forskellige handlinger, såsom massefilomdøbninger og filgendannelser.

Rådgivning om alle vores produkter, etablering af løsninger og opgradering af løsninger.

Ring til os på **89 80 80 89**

04. Aktiver SPF, DKIM og DMARC

Domain-based Message Authentication, Reporting and Conformance (**DMARC**) er et regelsæt for virksomhedens udgående e-mails, der verificerer afsenderens identitet. Dermed beskyttes dine kunder mod falske e-mails afsendt fra din virksomhed.
Ved at verificere virksomhedens indgående emails med DMARC, opnår man samtidigt at virksomheden beskyttes mod svindel emails, derunder spoofing og phishing.

DMARC protokollen gør brug af et sæt eksisterende og nye mekanismer for validering af emails, derunder **SPF** (Sender Policy Framework) og **DKIM** (Domain Keys Identified Mail). Dette kan give virksomheden et løbende overblik over, hvem der forsøger at sende e-mails på vegne af virksomhedens domæner; disse informationer kan benyttes til at opnå kontrol over, hvem der sender på vegne af virksomheden.

DKIM, SPF og DMARC kan kun blokere for falske e-mails sendt fra dine konti, hvis de er konfigureret korrekt. Vær derfor sikker på at regler og politikker for Microsoft 365 email sikkerhed er opsat korrekt for samtlige af virksomhedens domæner, herunder fuld **DMARC** policy i DNS mm. Du kan også bruge Centera **DMARC** Compliance og Valimail, som er monitoreringsværktøjer, der overvåger og varskoer, såfremt misbrug forsøges i din virksomhed.

Jo flere, der anvender DMARC korrekt, jo større er virkningen. I Danmark oplæves et stigende krav fra myndighedernes side med hensyn til at implementere DMARC. Alle statslige myndigheder er således blevet pålagt at implementere DMARC i en restriktiv politik.

Eftersom mere end 90% af alle IT-sikkerhedsrelaterede angreb starter med en eller flere e-mails fra de kriminelle, har din virksomhed brug for **DMARC** for at beskytte mod disse angreb. Desuden ønsker enhver virksomhed naturligvis, at deres kunder ikke modtager falske e-mails fra virksomheden.

DMARC står for:
Domain Message Authentication Reporting & Conformance, der som standarden for ægthedsvalidering af emails, sikrer at en email rent faktisk kommer fra den reelle indehaver af den angivnede email adresse.

Rådgivning om alle vores produkter, etablering af løsninger og opgradering af løsninger.

Ring til os på **89 80 80 89**

05. Få advarsler om mistænkelige aktiviteter

Microsoft 365 Security and Compliance Center kan identificere dine risici ved at lagre data og giver overblik over, hvorvidt dit firma opfylder jeres egne sikkerhedspolitikker bl.a. GPDR. Her er mange forskellige værktøjer, der kan hjælpe dig med sikkerheden.

Husk jævnligt at gennemgå, konfigurere og justere de relevante sikkerhedsindstillinger.

I Security and Compliance Center kan du slå bruger- og administratoraktivitetsovervågningen til. Unormal bruger- eller systemadfærd kan indikere et forestående eller fremadskridende angreb og bør straks rapporteres til de ansvarlige administratorer.

Stop

BEDRAGERIFORSØG

OG AVANCEREDE TRUSLER FRA EMAILS

Machine Learning kombineret med datafeeds fra både global og regional Cyber Threat Intelligence er grundlaget for en effektiv analyse og blokering af e-mails igennem Email Defence for Microsoft 365.

IT-kriminelle benytter ofte de mest udbredte sikkerhedslag som sandkassetest for at deres kampagner når tiltænkte mål.

Ved både at øge analysegrad, metoder og tilføre regionale efterretninger om målrettede kampagner, øges virksomhedens email sikkerhed væsentligt.

06. Brug Microsoft 365 Secure Score

Microsoft 365 Secure Score måler din organisations samlede sikkerhedstilstand på dine Microsoft 365-tjenester. Når du logger på Secure Score kan du se i procent, hvor mange sikkerhedsindstillinger der er i brug.

Værktøjet giver også praktiske anbefalinger til at lukke sikkerhedshuller og du kan se den maksimale score for din organisation. Du kan også se, hvordan din organisations score er, sammenlignet med den gennemsnitlige score på tværs af alle Office 365-kunder.

Den globale administrator for virksomhedens O365 har adgang til Microsoft365 Secure Score og kan dermed løbende give en indikation af virksomhedens sikkerhedstilstand.

07. Krypter virksomhedens e-mails

Som tidligere nævnt indeholder e-mails ofte følsomme oplysninger, herunder personlige oplysninger, betalingsdata og virksomhedshemmeligheder og disse oplysninger kan falde i de forkerte hænder, hvis en e-mail-konto er kompromitteret eller der opstår en fejl under overførslen.

E-mail-kryptering sikrer, at kun den rigtige modtager kan få adgang til den påtænkte besked og vedhæftede filer. Med de indbyggede e-mail-krypteringsfunktioner kan du indstille e-mails til at bede om en engangsadgangskode, når de åbnes.

Bruger du O365 kan du også vælge, at e-mailen kun kan læses i Office 365 og du kan begrænse kopiering og udskrivning.

Rådgivning om alle vores produkter, etablering af løsninger og opgradering af løsninger.

Ring til os på **89 80 80 89**

08. Aktiver tilføjelsesprogrammet Rapportmeddelelse

Tilføjelsesprogrammet Rapportmeddelelse giver dine brugere mulighed for at rapportere mistænkelige e-mails til Microsoft. Det er også her, du administrerer, hvordan din Microsoft 365 konto behandler disse meddelelser.

Ved at aktivere tilføjelsesprogrammerne Rapporter meddelelse og Rapporter phishing til Outlook kan dine brugere rapportere uønsket mail, såsom spam- og phishing-mails, hvilket kan være med til at forbedre Microsofts spamfiltre. Disse meddelelser vises i sikkerhedskontrolpanelet, for at give administratorer mulighed for at følge op eller handle, før de samme phishing-e-mails sendes til andre brugere og forårsager skade.

09. Uddan dine medarbejdere

En virksomheds IT-sikkerhedspolitik bør først og fremmest fokusere på, at lære medarbejderne at gebærde sig på internettet. Medarbejdere er normalt det svageste sikkerhedsled i enhver organisation. Menneskelige fejl tegner sig for 88% af databrud og er blandt de hurtigst voksende cybersikkerhedstrusler i dag. Et enkelt forkert tryk på en vedhæftet fil eller andet kan have alvorlige konsekvenser. Menneskelige fejl kan også ske for chefen.

Medarbejdere kan begå uskyldige fejl, negligere sikkerhedsprotokoller eller uforvarende falde for social engineering-svindel. Det mest sikre er at oprette et medarbejdertræningsprogram med fokus på bedste praksis for cybersikkerhed og sikkerhedsansvar for at minimere brugerrelaterede cyberrisici. Gennemgå og evt. opdatér medarbejdernes awareness-træning med henblik på at beskytte virksomheden mod social engineering, phishing og ransomware-angreb. Et enkelt kursus i cybersikkerhed er ikke nok – medarbejdernes viden skal jævnligt opdateres igennem awareness-træning.

Veluddannede medarbejdere er virksomhedens bedste mulighed for at forhindre cyberangreb og selv hvis medarbejderne måske ikke føler, at det er deres ansvar, er det nødvendigt at gøre klart, at det er det.

Uddan alle i at bruge passwords korrekt.

Læs mere i afsnit 10.

10. Password sikkerhed

Brug kun et password!
- men det skal være et rigtigt password.

Forebyggelse er essentielt og det anbefales, at alle brugere, kun har et password, som de kan udenad. Kodeordet skal være mellem 12 og 16 karakterer, indeholde store og små bogstaver, tal og mindst et specialtegn. Dette **password** skal IKKE skiftes, som det ofte har været anbefalet fra mange store organisationer. Dette er dog ved at ændre sig, og Microsoft anbefaler nu samme politik.

Et stærkt **password**, et som overholder reglerne for stærke password (se herunder). Sammen med MFA giver det virksomheden den bedste mulige sikkerhed, frem for at bede medarbejderne forny deres password hver 3. månede.

Brug disse retningslinjer for et godt password, så er passwordet markant stærkere end med password der skiftes hver 3. måned.

1. Mindst 12 karaktere gerne 16
2. Brug STORE og små bogstaver
3. Brug tal
4. Brug mindst en specialkarakter.

Eksempler på stærke **passwords**, som ikke skal fornyes hvis det bruges sammen med MFA.

Gode passwords der kan udtales	Gode password med vilkårlig karakter
0sp44VesterG4de386	aGV#928393O#IyPk
JoN4s&Kirten!4€v€r	5Dy9^NULJS62@2WR
A41b0Rg#SÆby	77V!Ae22@HnssR6h
Odd4r”k04benHavN	k4TsmMCbp#urPd66
Br0ndby@&V€sT€gn€n	28@tJA926!fG

Eller brug en adgangskodeadministrator, med en 2 faktor godkendelse på smartphonen.

SAC·IT
INSTANT TECHNOLOGY

I dette whitepaper er der brugt kilder fra
Statslige myndigheder om DMARC, Stanford og Microsoft.