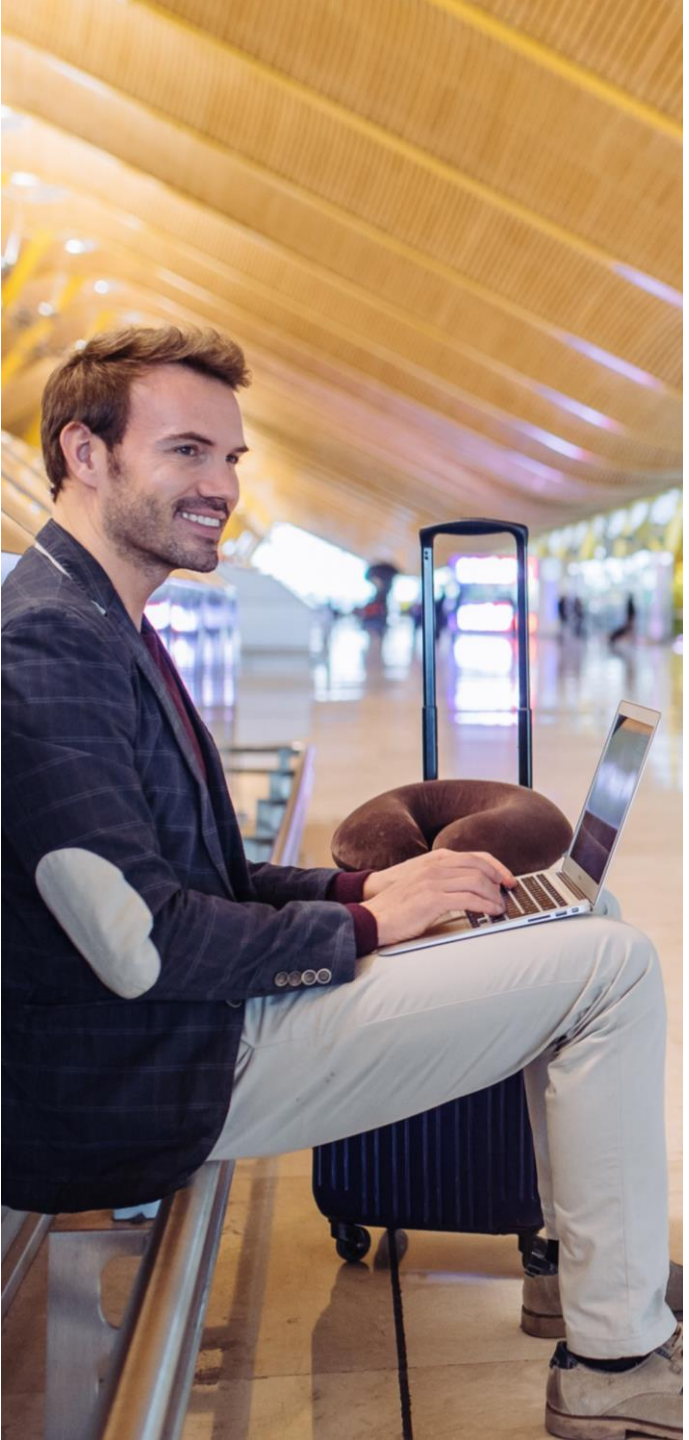
GUIDE
Microsoft 365 Sikkerhed

MINDCORE



Indhold

1. Principperne for moderne IT Sikkerhed
2. Typiske overvejelser omkring IT Sikkerhed
3. Sikkerhedsfunktioner i Microsoft 365
4. Fokuser på de rigtige sikkerhedstiltag
5. Kom videre med Microsoft 365 Sikkerhed
6. Vil du vide mere? Link til mere viden fra den tekniske verden

Principperne for moderne IT Sikkerhed

Corona-pandemien har medført at mange af os arbejder hjemmefra, hvilket har tvunget flere virksomheder til at forlade den klassiske tankegang om perimeteren som den sikre skanse og i stedet fokusere på zero-trust modellen hvor sikring af den enkelte brugers identitet, brugerens arbejdsstation og virksomhedens data er i fokus.

Men hvad er principper for Zero Trust modellen egentligt?

VERIFICY EXPLICITLY

Hvis jeg ikke stoler på noget, så skal alt verificeres

GIVE LEAST PRIVILEGED ACCESS

Giv mig kun den adgang der skal til for at jeg kan løse opgaven

Just-in-time-Access (JIT)
Just-enough-Access (JEA)

ASSUME BREACH

Tænk altid i at segmentere, kryptere og opdag trusler

I den moderne verden med hybridmiljøer, applikationer i skyen, hjemmekontorer mv. foregår deling af data i stigende grad over internettet. Det stiller andre krav til sikkerheden og det er her Zero Trust modellen giver værdi.

Zero Trust modellen bygger grundlæggende på 3 hovedprincipper (se nedenfor). Hvordan en virksomhed efterlever dette vil variere fra virksomhed til virksomhed, men grundlæggende handler det om et stærkt øget fokus på at sikre data, brugere og de enheder de arbejdet på.

Moderne sikkerhedsprincipper bygger på, at sikre den enkelte brugers identitet, brugerens arbejdsstation og virksomhedens data

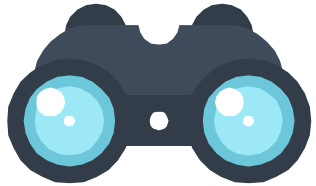
Typiske overvejelser virksomheder har om IT Sikkerhed

Får jeg nok sikkerhed for pengene?

Investeringen i Microsoft licenser er for mange virksomheder både dyr og vanskelig. Der findes en myriade af licenspakker der giver adgang til forskellige sikkerhedsfeatures. Derfor stiller mange virksomheder de samme to spørgsmål.

Får jeg nok sikkerhed for den investering jeg allerede har lagt?
Ofte har virksomheder adgang til langt flere sikkerheds-funktioner end de reelt bruger, og virksomheder bør starte her inden de overvejer yderligere investeringer.

Har jeg brug for at investere i flere licenser, og i givet fald hvilke?
Det er vigtigt altid at vurdere hvor meget mere sikkerhed virksomheden får ved at investerer i yderligere licenser. Skal virksomheden investere så skal de investere i det som giver mest sikkerhed for pengene.



Hvor skal jeg lægge indsatsen?

Med de omfattende muligheder der er indenfor sikkerhed omkring identitet, data og enheder er der mange virksomheder der er udfordret på at beslutte hvilke sikkerhedsfunktioner de bør implementere.

Her bør virksomheden for hver sikkerhedsfunktion overveje følgende:

Modenhed: Hvor moden er den pågældende funktion? Er det en ny eller gennemtestet funktion fra Microsoft?

Implementeringsomfang: Hvor mange ressourcer kræver det at implementerer den pågældende sikkerhedsfunktion?

Brugerpåvirkning: Hvad er konsekvensen for den enkelte bruger/brugeroplevelse?

Sikkerhedsgevinst: Hvor meget ekstra sikkerhed vil den pågældende funktion reelt give virksomheden?

Sikkerhedsfunktioner i Microsoft 365

Der findes rigtig mange sikkerhedsfunktioner på tværs af Microsofts mange licenspakker. Nedenfor en oversigt over centrale sikkerhedsfunktioner fordelt på Klienter, Identiteter, Data & Governance og Øvrige.

KLIENTER

- AppLocker
- Attack Surface Reduction (ASR)
- BIOS Settings and lockdown
- BIOS updates
- Bitlocker
- Bitlocker To Go
- Certificates in the Intranet zone
- Microsoft Endpoint Data Loss Prevention (DLP)
- Desktop Analytics
- Device Guard
- Direct Memory Access (DMA) protection
- Endpoint Analytics
- Firmware control (TPM, AMT, BIOS)
- Internet based management
- Microsoft Defender for Endpoint
- Microsoft Endpoint Manager (MEM vs. MECM)
- Microsoft/Office Security Compliance Toolkit (SCT)
- Monitoring and compliance – Patch management
- Monitoring and compliance – Security solutions
- Office 365 Channel control
- Patch management - 3. party applications
- Patch management – Microsoft
- Public Key Infrastructure (PKI)
- Secure Boot
- Server Message Block (SMB) signing
- Smart cards
- Tier model (isolation)
- Trusted Platform Module (TPM) versions
- Unified Extensible Firmware Interface (UEFI)
- Update compliance
- Virtual smart cards
- Virtualization Based Security (VBS)
- Windows Channel control
- Windows Defender Application Guard
- Windows Defender Exploit Guard
- Windows Hello for Business
- Windows Sandbox
- Workstation Hardening

IDENTITETER

- AD users and workstations not in use
- Azure AD Access Reviews
- Azure AD Entitlement Management
- Azure AD Identity Protection
- Azure AD Password Protection and Smart Lockout
- Azure Role-Based Access Control (RBAC)
- Conditional Access
- Credential Guard
- Domain admins
- Local Administrator Password Solution (LAPS)
- Microsoft Defender for Identity
- Multi-Factor Authentication (MFA)
- Password never expires
- Password-less sign-in
- Password-less Authentication in Azure AD
- Privileged Access Management (PAM)
- Privileged Identity Management (PIM)
- Protected Users Security Group
- Self Service Password reset

DATA & GOVERNANCE

- Microsoft Defender for Office 365
- Microsoft Information Protection (MIP)
- Sensitivity Labelling
- Office 365 Data Loss Prevention (DLP)
- Office 365 Message Encryption (OME)
- Office Macros
- Insider Risk Management
- Office365 Security and Compliance

ØVRIGE

- Advanced Threat Analytics
- Azure Bastion
- Azure Just-In-Time (JIT) virtual machine access
- Azure Secure Score
- Azure Security Center
- Azure Sentinel
- Customer Lockbox
- Customer Keys
- Insider Risk Management Analytics
- Lightweight Directory Access Protocol (LDAP) signing
- Log Analytics

MINDCORE

4 centrale sikkerhedstiltag der skaber et stærkt grundlag for at sikre din virksomhed

Fokusér på de rigtige sikkerhedstiltag fra starten

Enhver virksomhed der arbejder med sikkerhed, hvad end man starter fra begyndelsen eller bygger videre på eksisterende sikkerhedsfunktionalitet, bør sikre, at disse fire centrale sikkerhedstiltag er adresseret.

BESKYT BRUGERNES IDENTITET

Multi Factor Authentication (MFA)

Conditional Access

Identity Protection

OPDATER OG BESKYT DINE ENHEDER

Endpoint Manager & Configuration Manager

Endpoint protection

Endpoint data loss prevention

BESKYT DE ADMINISTRATIVE PRIVILEGIER

Privileged Identity Management

Privileged access groups

Role-based Access Control (RBAC)

BESKYT DATA OVERALT

Sensitivity labelling

Data loss prevention (DLP)

Insider risk management

MINDCORE

En struktureret måde at komme videre med M365 Sikkerhed

Få konkret inspiration, sparring og anbefalinger til hvordan du kan kommer videre med IT Sikkerhed på Microsoft platformen gennem Mindcore's M365 sikkerhedsworkshop.

Formål

Formål med workshoppen er, at give indsigt i sikkerheds-funktionalitet på Microsoft platformen, som input til at øge sikkerhed på eksisterende platform og give konkrete anbefalinger til at komme vider med virksomhedens IT Sikkerhed

Resultat

Baseret på virksomhedens ønsker og behov gives dyb indsigt, og inspiration om relevant M365 sikkerheds-funktionalitet. Workshoppen er målrettet og dialogbaseret og resultatet er konkrete sikkerheds-anbefalinger der kan implementeres.

Relevans

Workshoppen er relevant for alle niveauer i virksomheden, fra IT og driftsdirektøren der ønsker inspiration og sparring på de store linjer, til arkitekten og specialisten der ønsker dyb indsigt og sparring på konkret funktionalitet. Den ønskede vinkling aftales på forhånd.

Omfang

Inspirationsworkshoppen varer ca. 3-5 timer. Eneste forudsætning er et kort formøde til afstemning, samt at virksomheden stiller med relevante personer på dagen, der kender til virksomhedens udfordringer og som ønsker konkret inspiration og sparring

Typisk forløb for gennemførsel af Mindcore M365 Sikkerhedsworkshop

1 AFSTEM FOKUS

Formøde hvor vi afstemmer virksomhedens ønsker til workshoppen - herunder konkrete fokusområder og sikkerhedskomponenter

(ca. 1 time)

2 SIKKERHEDS WORKSHOP

Sikkerhedsworkshop hvor vi går i dybden med aftalte sikkerhedsområder og giver konkret inspiration, sparring og anbefalinger

(8-10 timer, inkl. forberedelse)

3 RAPPORT UDARBEJDES

Udarbejdelse af sikkerhedsrapport med heatmap og konkrete konklusioner og anbefalinger

(ca. 1 dag)

4 ANBEFALINGER PRÆSENTERES

Opsamling fra workshop, hvor der udarbejdes en sikkerhedsrapport med konkrete anbefalinger der præsenteres for virksomheden

(1-2 timer)

MINDCORE

Hvad kommer der ud af Mindcore's M365 Sikkerhedsworkshop?

Workshoppen er konkret og fokuseret på, at give indsigt, overblik og klare handlingsrettede anbefalinger til at komme videre. Konkret udmunder workshoppen i tre leverancer

M365 Sikkerhedsrapport

Rapporten indeholder en gennemgang af workshoppens konklusioner og anbefalinger herunder;

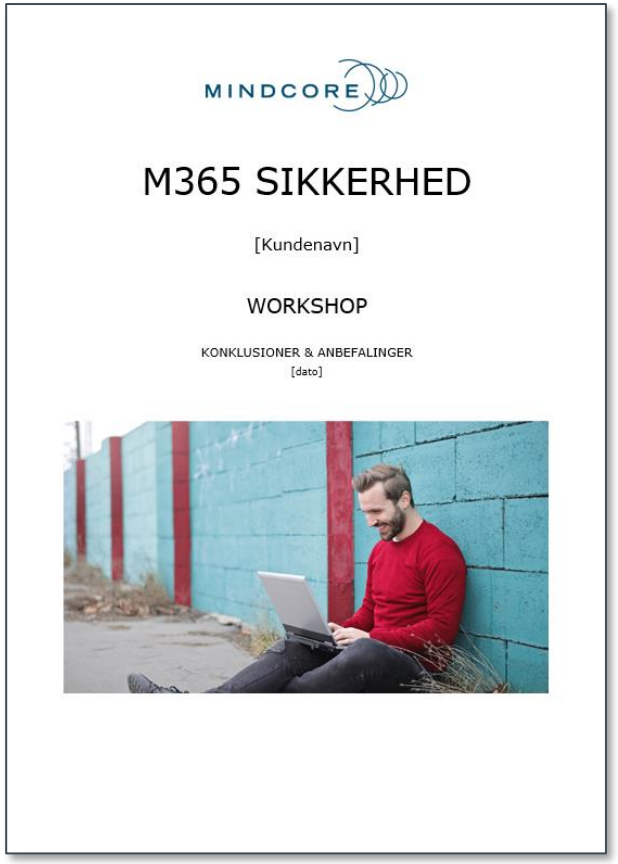
- ✓ Kort beskrivelse af de anbefalede sikkerhedsfunktioner
- ✓ Anbefalinger/overvejelser omkring implementering
- ✓ Licenskrav

M365 Sikkerhedsheatmap

Heatmap dækker de sikkerhedsfunktioner som indgår i workshoppen, og er prioriteret efter funktionens modenhed, implementeringsomfanget, brugerpåvirkning og sikkerhedsgevinsten for virksomheden.

Præsentation af Sikkerhedsrapport

Konklusioner og anbefalinger præsenteres for kunden ved gennemgang af rapport og heatmap, herunder en drøftelse af et eventuelt videre forløb.



MINDCORE

Vil du vide mere? Link til mere viden fra den tekniske verden

Mindcore Teknisk Blog udgiver dybdegående tekniske artikler om Infrastruktur, Sikkerhed, Klient Administration og Cloud.

Artiklerne nedenfor relaterer sig til Microsoft 365 sikkerhed og der bliver løbende udgivet nye tekniske artikler.

Password-less phone sign-in with the Microsoft Authenticator app: https://blog.mindcore.dk/2019/04/password-less-phone-sign-in-with_8.html

Windows Defender Application Guard – Settings: https://blog.mindcore.dk/2019/02/windows-defender-application-guard_25.html

Azure AD Password Reset on login screen: https://blog.mindcore.dk/2019/03/azure-ad-password-reset-on-login-screen.html

Windows Defender Application Guard: https://blog.mindcore.dk/2019/02/windows-defender-application-guard.html

Manage security polices directly from the cloud without co-management: https://blog.mindcore.dk/2020/11/manage-security-polices-directly-from.html

Microsoft Endpoint Analytics – Proactive remediations: https://blog.mindcore.dk/2020/08/microsoft-endpoint-analytics-proactive.html

How to activate app lock on Microsoft Authenticator app: https://blog.mindcore.dk/2020/08/how-to-activate-app-lock-on-microsoft.html

Block non-compliant devices from syncing corporate data using OneDrive: https://blog.mindcore.dk/2020/06/block-non-compliant-devices-from.html

Restrict the ability to Edit documents in Microsoft Teams: https://blog.mindcore.dk/2020/06/restrict-ability-to-edit-documents-in.html

Governance and compliance in office365 – part 1: https://blog.mindcore.dk/2020/05/governance-and-compliance-in-office365.html

Automatic bitlocker installation on Windows 10: https://blog.mindcore.dk/2020/04/automatic-bitlocker-installation-on.html

Defender tamper protection: https://blog.mindcore.dk/2020/04/defender-tamper-protection.html

Mindcore Teknisk Blog

https://blog.mindcore.dk

Hvis du vil høre mere

· MINDCORE ·
Lottenborgvej 26A, 2. sal – 2800 Kongens Lyngby

Michael Nielsen

Sikkerhedskonsulent
E-mail: mn@mindcore.dk
Mobil: +45 31 31 92 44

Jacob Guldager-Løve

Partner
E-mail: jgl@mindcore.dk
Mobil: +45 52 15 01 14

MINDCORE