Codeex Care

Endpoint

- fuld kontrol og tryghed i din IT-drift

Integrating IT

codeex

Effektiv administration og systematisk sikkerhedsopdatering giver mere tid til udvikling

I en cloud-baseret verden skal der opdateres hurtigere og oftere end tidligere. Derfor er det afgørende at have en systematisk tilgang til IT-administration og sikkerhedsopdateringer.

Med Codeex Care Endpoint får I en partner, der fungerer som jeres support-, drifts- og sikkerhedsafdeling, så i får mere tid til at understøtte forretningens strategiske mål. Udover opsætning og vedligeholdelse sikrer vi også, at jeres løsning fortsat leverer værdi gennem compliance, optimering og effektiviseringer.

Codeex Care Endpoint er baseret på Microsoft 365 og de muligheder, som Microsoft 365 suiten tilbyder. Herunder blandt andet håndtering og support af brugere, mail, enheder, data, sikkerhed, compliance – og meget mere.

Altid informeret
Hvert kvartal holder vi et statusmøde. Her gennemgår vi de vigtigste hændelser, evt. nye initiativer og hvad der kommer til at ske fremover. Desuden kommer vi med forslag til, hvordan I kan få endnu mere værdi ud af jeres IT-setup i hverdagen.

Fordelene

- **Automatisering og effektivitet:** Alle enheder administreres automatisk via Intune og Autopilot, så I sparer tid og ressourcer.
- **Maksimal datasikkerhed:** Avancerede sikkerhedspolitikker og compliance sikrer jeres data mod interne og eksterne trusler.
- **Reducerede driftsomkostninger:** Optimering af cloud-miljøet giver mulighed for at nedskalere fysisk infrastruktur og undgå uforudsete udgifter.
- **Løbende support og opdatering:** Vores team overvåger og vedligeholder jeres løsninger kontinuerligt, så de altid er opdaterede.

Hvorfor vælge Codeex Care Endpoint?

Med Codeex Care Endpoint får I ikke blot en service. I får en aktiv strategisk partner, der sikrer, at jeres IT-drift er robust, sikker og altid up-to-date. Vi tager ansvaret for administration og sikkerhed, så jeres virksomhed kan fokusere på det vigtigste: At vækste.

Codeex Care Endpoint sikrer:

Brugerkonti og grupper

- Oprettelse og nedlæggelse af brugere.
- Tildeling og fjernelse af rettigheder.
- Oprettelse og nedlæggelse af grupper, herunder styring af medlemskaber.
- Opsætning og vedligeholdelse af multifaktorgodkendelse (MFA) for alle brugere.
- Andet vedligehold af brugere og grupper.

Mail

- Oprettelse og nedlæggelse af bruger- og delte postkasser.
- Sikring af mailflow gennem korrekt opsætning af SPF, DKIM og DMARC.
- Mulighed for kryptering af udgående mails.
- Verificering af mistænkelige mails ved tvivl om skadelig indhold.

Data og kommunikation

- Opsætning og strukturering af SharePoint og Teams for optimal datasikkerhed og samarbejde.
- Begrænsning af adgange til sensitive data og kontrol med oprettelse af nye teams.
- Automatisk udrulning af Windows 10/11 via Autopilot.
- Automatisk nulstilling eller sletning af registrerede enheder ved tyveri.

Sikkerhed

- Implementering af Microsoft Defender Endpoint for avanceret beskyttelse mod malware, phishing og andre trusler.
- Opsætning af sensitivity labels for datasikkerhed.
- Kryptering af alle enheder med Microsoft BitLocker.
- Compliance-monitorering og optimering af secure score i Microsoft 365.
- Udrulning af sikkerhedsbaselines i henhold til Microsofts anbefalinger.

Løbende support og vedligehold

- Automatisk opdatering af operativsystemer og software.
- Overvågning og fjernelse af sikkerhedstrusler i realtid.
- Kvartalsvise statusmøder hvor vi gennemgår forbedringsforslag og kommende opdateringer.
- Hjælp til opsætning af politikker der beskytter enheder og data.

En løsning, der støtter både medarbejdere og strategi

Bilag 1

Etablering

Oprettelse af Microsoft 365 tenant
- Hvis tenant eksisterer, gennemgås denne og der implementeres de nødvendige tiltag for at sikre tenanten.

Håndtering af licenser

Oprettelse af brugere, postkasser og ressourcer i samarbejde med kunden
- Hvis tenant eksisterer, laves der oprydning i ovenstående i samarbejde med kunden

Konfiguration af Intune til enhedshåndtering:
- Konfigurations- og sikkerhedspolitikker
- Opdateringspolitikker
- App-pakker til kundespecifikke applikationer (fx NAV, softphones, TeamViewer el.lign.)
- Autopilot til automatisk opsætning af Windows-enheder

Konfiguration af følgende sikkerhedsfunktioner henvendt mod brugeren:
- "Strong authentication" (MFA, passwordless, FIDO2 m.fl.)
- Self Service Password Reset (SSPR)
- Device compliance

Konfiguration af SPF, DKIM og DMARC for sikring af mailflows

Udsendelse af informationsbrev til slutbrugerne

Indhold

Fri brug af Codeex support:
- Kontakt via mail eller telefon
- Oprettelse, nedlæggelse og ændring af brugere
- Genoprettelse af brugere i Microsoft 365 (herunder mail og OneDrive data) i op til 30 dage efter sletning
- Hjælp til fejlretning af tjenester:
  - Microsoft 365 herunder tenant, licensering, tilgange og andre tjenester
  - Evt. synkronisering mod Active Directory i en hybrid opsætning
  - Operativsystem og Microsoft 365 applikationer
  - Oprettelse af supportsager hos Microsoft
  - Garantisager for enheder

Exchange Online
- Oprettelse og drift af delte postkasser, mødelokaler, grupper og transportregler
- Drift af SPF, DKIM og DMARC
- Drift af spamfilter

SharePoint/Teams
- Oprettelse og drift af grupper og indstilling af korrekte rettigheder
- Oprettelse og drift af gruppe hvor kun medlemmerne kan oprette SharePoint sites eller teams
- Begrænsning af delingsrettigheder med eksterne efter aftale med kunden ud fra et sikkerhedsperspektiv

Entra

- Administration af brugere, grupper og enheder
- Opsætning og vedligehold af Azure AD sync (hvis on-premise AD benyttes)
- Registrering af enterprise applications og opsætning af app registrations
- Opsætning af "app request and consent"-flow, og deaktivering af muligheden for at registrere applikationer, som kræver andre rettigheder end et forudbestemt sæt, der har minimal indvirkning på sikkerhed
- Opsætning af virksomhedsbranding (med materiale udleveret af kunden)
- Konfiguration af følgende conditional access politikker:
  - Aktivering af strong authentication for alle brugere
  - Begrænsning så MFA kun kan opsættes fra bestemte lokationer
  - Blokering for adgang fra enheder, der ikke opfylder compliance krav
  - Blokering af udfasede protokoller til godkendelse
  - Begrænsning af SMTP-protokol til udvalgte lokationer
  - Begrænsning for mobile enheder til kun at kunne benytte Microsoft-applikationer for at tilgå virksomhedsdata
- Aktivering af Self-Service Password Reset (SSPR) så brugere selv kan nulstille deres adgangskoder

Intune

- Enhedshåndtering, opsætning og vedligehold af:
  - Autopilot
  - Nulstilling af enheder
  - Codeex' konfigurationspolitikker
  - Codeex' sikkerhedsbaseline
  - Diskkryptering (BitLocker)
  - Apple Business Manager
  - Google Enterprise
- Applikationer:
  - Oprettelse og opdatering af applikationspakker
  - App beskyttelses- og konfigurationspolitikker
- Automatisk opdatering af OS på enheder
- Opsætning og vedligehold af compliance-politikker

Compliance og sikkerhed

- Konfiguration af sensitivity labels
- Aktivering og opsætning af DLP-politikker efter behov
- Aktivering af revisionslogs:
  - Gennemgang af revisionslogs efter forespørgsel
- Beskyttelse mod eksterne trusler med Microsoft 365 Defender:
  - Anti-phishing
  - Anti-spam
  - Anti-malware
  - Safe attachments
  - Safe links
  - ASR (Attack surface reduction)
  - Controlled folder access
  - Network filtering
  - Exploit protection
- Gennemgang og vedligehold af secure- og compliance-score