Azure Security
Tjekliste
24 tjekpunkter du kan bruge til at
booste sikkerheden i Azure på rekordtid
SAC·IT
INSTANT TECHNOLOGY
×
Azure

Vi bringer en advarsel

Sikkerhedsbrud i Azure kan få store konsekvenser for dig. Ifølge Microsoft hænger du på regningen, hvis kriminelle hacker dig og udnytter din Azure-konto.

Microsoft Azure vokser med rekordfart. Det samme gør udviklingen af platformen og potentielle udfordringer med sikkerheden.

Derfor er det essentielt for dig som it-partner eller kunde at forstå, hvad du har ansvaret for i Azure, samt du kan gøre for at styrke sikkerheden.

Alt sammen får du hjælp til her! Med vores tips og tjeklister til Azure kan du minimere risikoen for at miste penge, data og omdømme.

Indhold:

- ***Hvad er Azure Shared Responsibility?***
- ***Hvem har ansvaret i Azure?***
- ***Hvor galt kan det gå?***
- ***Azure security tjekliste***
- ***Reminder***

Azure Shared Responsibility

Hvad har du ansvaret for i Azure? Hvad skal Microsoft? Mange er i tvivl, og derfor skal du kende Azure Shared Responsibility-modellen, som forklarer ansvarsfordelingen.

Microsoft Azure's ansvar

Det er Microsofts ansvar at sikre servere og det fysiske netværk.

Azure har fokus på sikkerheden i den underliggende infrastruktur og beskytter mod uautoriseret adgang til blandt andet computing, storage, netværk og database.

Microsoft er selvfølgelig også ansvarlig for sikkerheden for sine fysiske datacentre med Azure services, samt dens software og hardware.

Afslutningsvis tager Azure sig også af sikkerheden for managed services som fx SQL, Blob, Cosmos DB og Kubernetes.

Kundens ansvar

Det er kundens ansvar at sikre adgangs-kontrol og alt, der bliver anvendt og bygget i Azure.

Som Azure-partner eller kunde har du ansvaret for at beskytte "din egen" cloud, herunder alt du bygger og bruger i Azure.

Du skal bl.a. sørge for at sikre netværket, dine konti og brugere, samt sikkerhedskopiering af data og apps i Azure.

Du har også ansvaret for at aktivere MFA for alle Azure-brugere.

Hvem har ansvaret i Azure?

Azure Shared Responsibility-modellen i praksis:

Her er eksempler på ansvarsområder for kunden, it-partner og Microsoft Azure.

Opgaver	Kunde el. it-partner	Azure
Beskyttelse af adgangskoder og brugeridentiteter (fx MFA aktivering)	✔	—
Forebyg og identificér kompromitterede Azure-konti	✔	—
Sikkerhedskopiering og gendannelse af data og applikationer i Azure	✔	—
Begrænse adgang til Azure services og apps til godkendte brugere	✔	—
Sikker konfigurering af Azure services baseret på best practice	✔	—
Konfiguration og beskyttelse af virtuelle netværk og infrastruktur i Azure	✔	✔
Beskyttelse af data, der overføres mellem lokale systemer og Azure tjenester	✔	✔
Overholdelse af sikkerhedsregler og compliance for Azure-miljøet	✔	✔
Fysisk beskyttelse og sikkerhed af Azure datacentre og infrastruktur	—	✔
Overvågning og rapportering af sikkerhedsbegivenheder og -trusler i Azure	—	✔
Sikre tilgængelighed og ydeevne i Azure-tjenester og infrastruktur	—	✔
Sikre fysisk adgangskontrol til hardware og software	—	✔
Database patching	—	✔

Hvor galt kan det gå?

Eksempel: En dansk handelsvirksomhed bliver hacket, hvor cyberkriminelle får adgang til firmaets Azure-konto. Der er adgang til følsomme oplysninger, og der bliver bestilt dyre Azure resources, som giver kunden en astronomisk regning.

Hackerne får adgang til Azure-kontoen via en brugers login, som ikke er sikret med 2FA.

Loginoplysningerne er ganske nemme at kapre – via phishing, optagelse af tastetryk eller "gæt", hvis koden er svag eller genbrugt.

Hvem hænger på regningen?

Med adgang til kontoen opsætter hackerne automatiske scripts, som opretter dyre Azure resources på et splitsekund. CosmosDB, Blob Storage, Kubernetes og virtuelle netværk drøner derudaf. Og på den måde stiger kundens Azure-forbrug med over 100.000 kroner om dagen.

Hvem hænger på regningen? Det gør kunden, desværre, ifølge ***Microsofts betingelser***.

Angrebet bliver derfor meget dyrt for virksomheden, som på få, skæbnesvangre dage mister penge, data og omdømme.

Azure Security Tjekliste

På de næste sider kommer 24 konkrete tips til at styrke sikkerheden på din Azure-konto og beskytte dig mod hackere og uautoriseret adgang:

MFA

- ☐ Aktivér multifaktor-autentificering (MFA) på alle brugere
- ☐ Aktivér MFA på privileged accounts og overvej betingede adgangspolitikker (fx geo, IP-adresse, enhedstilstand osv.)
- ☐ "Enable users to memorize multifactor authentication on devices they trust" skal være deaktiveret
- ☐ "Require multifactor auth to join devices" skal være indstillet til "Yes"

Eksterne konti

- ☐ Sørg for, at der ikke er adgang for gæstebrugere
- ☐ "Guests can invite" skal være indstillet til "No"
- ☐ Giv ikke tilladelser til eksterne konti (dvs. konti uden for jeres subscription)
- ☐ "Users can consent to apps accessing company data on their behalf" indstilles til "No"
- ☐ Sørg for, at adgangen til Azure AD-administrationsportalen er begrænset
- ☐ Deaktiver RDP-adgang til netværkssikkerhedsgrupper fra internettet
- ☐ Deaktiver SSH-adgang til netværkssikkerheds-grupper fra internettet

Admins, Users og Roles

- ☐ Minimér antallet af admins/owners
- ☐ Brug Role-Based Access Control til alle admin konti i stedet for at tildele Global Administrator-rettigheder til alle privilegerede konti
- ☐ "Notify all admins when other admins reset their password" skal være indstillet til "Yes"
- ☐ "Members can request" skal være indstillet til "No"
- ☐ "Caution users on password resets" skal være indstillet til "Yes"
- ☐ "Users who can handle security groups" skal være indstillet til "None"
- ☐ Aktivér Privileged Identity Management for Privileged Roles
- ☐ "Number of days before users are asked to re-confirm their authentication report" må ikke være indstillet til 0
- ☐ "Number of processes required to reset" indstilles til 2

SQL-database og servere

- ☐ "Auditing type" skal være indstillet til "Blob" på SQL-servere
- ☐ "Auditing" skal være indstillet til "On" på SQL-database eller servere
- ☐ "Threat detection" skal være indstillet til "On" på SQL-database eller servere
- ☐ "Transparent data encryption" være indstillet til "On" på SQL-database eller servere

Reminder

Mange virksomheder antager, at Azure sørger for sikkerheden. Eller "dækker skaderne" efter et angreb. Disse fejlagtige antagelser har resulteret i mange fejl og sikkerhedsbrud, hvor hackere er stukket af med store summer penge og data. Sikkerhed i Microsoft Azure er baseret på Shared Reponsibility-modellen.

Microsoft sikrer servere og det fysiske netværk. Du skal til gengæld sørge for sikkerheden af følgende i Azure:

- ☐ Data og apps
- ☐ Endpoints
- ☐ Operativsystemer
- ☐ Konti og brugere
- ☐ Netværkskontrol
- ☐ Backup

Kontakt

Henning Plannthin
Head of Cloud
hep@sac-it.dk

Viktor Mikkelsen
IT Consultant / Cloud
vmi@sac-it.dk

Tlf: 89 80 80 00

www.sac-it.dk