Læsetid ca. 8 min.

IT-SIKKERHED I SKYEN

Zero trust – en ny måde at tænke it-sikkerhed på

timengo e-bog om it-sikkerhed
Udgivet juni 2019

timengo.
enter the cloud

Cloud ændrer alt

– også din it-sikkerhed

It-sikkerhed handler helt grundlæggende om, at give "the good guys" adgang og holde "the bad guys" ude.

Det har vi traditionelt set gjort ud fra en model, hvor vi med firewalls, virtual private networks og web gateways har bygget voldgrave og vindelbroer for at beskytte os. Og nøglen til at komme igennem dette panser, har været dit brugernavn og password!

Ifølge en af de største undersøgelser af faktiske databrud, Verizon Data Breach Investigation Report, involverer fire ud af fem databrud svage eller stjålne adgangskoder. Ligeledes anslår Forrester, at 80 procent af sikkerhedsbrud indebærer kompromitteret legitimationsoplysninger. På den baggrund tør vi godt konkludere, at en hacket "identitet" er en meget konkret angrebsfaktor. Og set i lyset af den hurtigt voksende digitalisering vil du kun blive yderligere udfordret. Flere og flere cloud baserede services,

In the age of digital transformation, **perimeters don't exist** and old approaches to security don't stack up against the sophistication of today's threats.

Dr. Chase Cunningham fra Forrester Research.

IoT enheder og mobile medarbejdere og enheder – tilsammen udvider det hackerens angrebsflade og sætter den traditionelle perimeterbaserede it-sikkerhed under pres. Du kan ikke længere stole på nogen eller noget, der identificerer sig alene på et brugernavn og password - heller ikke selvom de er inden for virksomhedens murer.

I e-bogen sætter vi fokus på, hvad cloud betyder for den måde, vi traditionelt har tænkt it-sikkerhed på og hvordan du i en moderne it-verden beskytter dig selv, virksomheden og dine kunder.

Rigtig god læselyst.

timengo.
enter the cloud

39 % af danske små og mellemstore virksomheder er **særligt sårbare** overfor it-sikkerhedsangreb

Det viser en rapport fra Erhvervsstyrelsen i 2018, som undersøgte it-sikkerhedsniveauet i små og mellemstore virksomheder (SMV'er). Deloitte Cyber Risk har siden 2012 gennemført flere hackersimuleringer på tværs af 550 danske virksomheder.

timengo.
enter the cloud

Indhold

Zero Trust

– et paradigmeskift

”Væk fra at tro, at vi kan lukke os inde og være sikre”

Accepter, at internettet er den fællesnævner vi alle sammen arbejder med. Du skal kunne drive din virksomheds it udelukkende ved at bruge internettet og uden at have dit eget netværk. Og måden du så får kontrol over din sikkerhed er ved, at identiteterne bliver beskyttet, dine data bliver beskyttet og de enheder, der tilgår de data og identiteter bliver beskyttet.

Martin Lundsgaard, Partner og CTO, timengo

Video

Se Martin Lundsgaard beskrive Zero Trust paradigmet som et resultat af, at internettet er kommet til at fylde mere og mere i virksomheders it.

timengo.
enter the cloud

Zero Trust

– en ny måde at tænke it-sikkerhed på

Traditionel it-sikkerhed bygger på en velafgrænset perimeter og antagelsen om, at alt inden for virksomhedens netværk er sikkert.

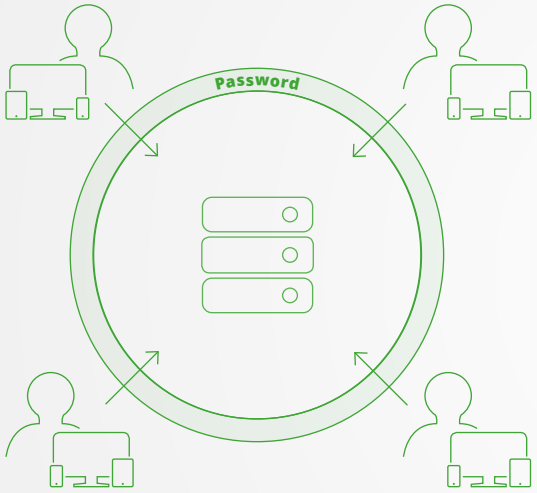
Glem det. I dag er data, applikationer, enheder og infrastruktur ofte hybride, cloud baseret og spredt uden for virksomhedens domæne – internettet er blevet "bærelinje" for dine data. Det betyder, at dit perimeter nu er der, hvor dine brugere og deres enheder er – og de kan være overalt!

Tillid er godt, kontrol er bedre

Zero Trust er en holistisk tilgang til it-sikkerhed, der evaluerer en sikkerhedstrussel ud fra princippet – "tillid er godt, kontrol er bedre".

Modellen er designet til at kontrollere en bruger ud fra den kontekst, han optræder i – fx hvilken enhed er han på, hvor er han placeret fysisk og hvilke data forsøger han at få adgang til. Med andre ord, Zero Trust er en brugercentreret sikkerhed, der tager flere datapunkter med i sin overvejelse i stedet for blot at spørge "Har du det rigtige password?"

Traditionel tilgang



Zero Trust tilgang

Den letteste måde at tænke Zero Trust på er at antage, at alt er på det åbne internet, selv ressourcer der ligger inden for dit domæne. Med Zero Trust flytter du tilliden fra kun at verificere ét enkelt element til i stedet at verificere på flere elementer ad gangen – brugeren, enheden og adfærden.

timengo.
enter the cloud

Tre vigtige trin mod en Zero Trust model

1 Validering af bruger

Hvordan kan du skabe brugerkontrol med MFA?

2 Validering af enhed

Skab kontrol af enheder med Device Management

3 Intelligent data- og adgangskontrol

Giv dine brugere en forudbestemt tilpasset adgang

timengo.
enter the cloud

1 Validering af bruger

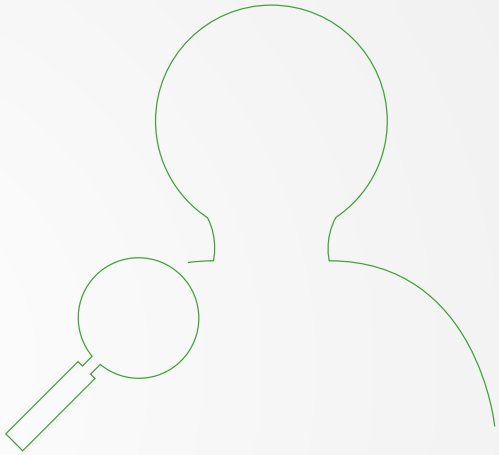
Hvordan kan du skabe brugerkontrol med MFA?

I en moderne it-organisation er dine brugere ofte på farten. De arbejder hjemmefra, er på kundemøder eller forretningsrejse. De tilgår forskellige cloud services, netværk og logger på fra forskellige enheder.

Et første og meget grundlæggende trin mod Zero Trust modellen er implementering af multi-factor-authentication (MFA).

MFA verificerer en bruger ved at kræve flere oplysninger i kombination med hans password, fx en kode fra hans smartphone, svaret på et sikkerhedsspørgsmål, et fingeraftryk eller en ansigtsgenkendelse.

Det er en effektiv måde at øge din sikkerhed på, fordi du ret enkelt kan kontrollere, at brugeren er den, han hævder at være, samtidigt med at du gør et stjålet password ubrugeligt for hackeren.



20 procent af virksomhederne nævner, at en læk af forretningskritiske data vil betyde, at de mister deres forretningsgrundlag og **potentielt må dreje nøglen om**

timengo.
enter the cloud

2 Validering af enhed

Hvordan kan du skabe kontrol af enheder med Device Management?

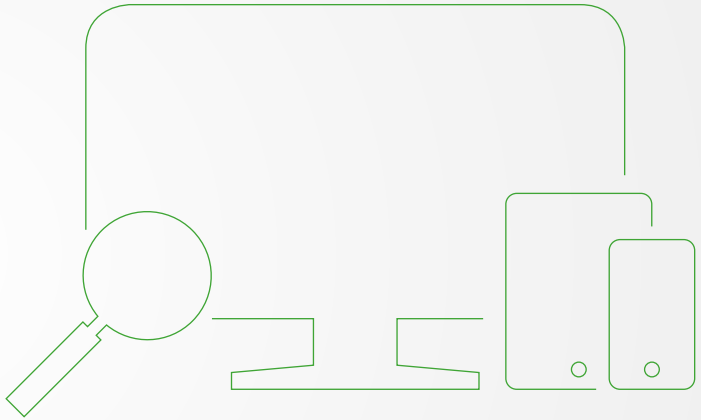
Ligesom cloud giver mulighed for, at vi arbejder mere mobilt i dag end tidligere, så er vi også blevet mere fleksible i forhold til, hvilke enheder vi tilgår virksomhedens data og systemer fra. Flere og flere virksomheder tillader og endda opmuntrer til at, medarbejdere kan medbringe deres egne enheder.

Den tilgang betyder, at du må vurdere hver enhed, der forsøger at tilgå dit netværk.

Ligesom MFA validerer en bruger, kan du med Device Management værktøjer opsætte forskellige betingelser for dine brugers adgange og adfærd på bestemte enheder ud fra en bestemt kontekst.

Er enheden administreret af virksomheden eller medarbejderen? Har enheden tidligere fået adgang? Har den korrekt software og opdateringer installeret? Og opfylder den dine sikkerhedspolitikker? Det er bare for at nævne nogle få.

Enheder, der ikke er styret af virksomheden eller overholder dine politikker, kan du ikke stole på. De bliver enten låst ude eller får et meget begrænset adgangsniveau.



3 Intelligent begrænset adgang

Giv dine brugere en forudbestemt tilpasset adgang

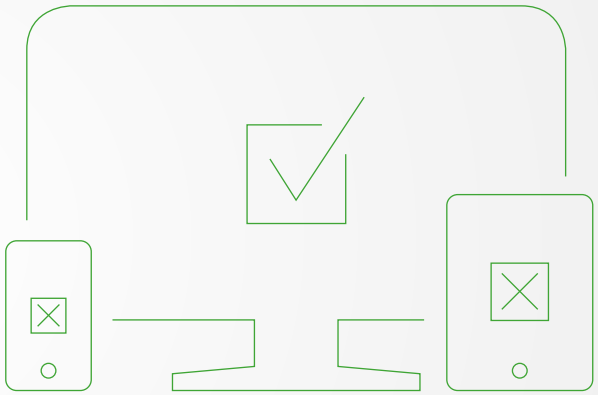
Det sidste trin i Zero Trust modellen handler om at forstå, hvem der bruger virksomhedens ressourcer og give dem en forudbestemt tilpasset adgang.

Det handler om governance og bevidst at tage stilling til, hvad dine brugere skal have adgang til, for at de kan udføre deres arbejde optimalt.

- Skal dine brugere fx have rollebaserede, rettighedsbaserede eller tidsbestemte adgange?
- Hvad må brugeren gøre med data; læse, redigere, printe, downloade?
- Fra hvilke typer enheder kan brugeren tilgå apps og data?
- Skal du kunne trække data tilbage, hvis en bruger ikke længere skal have adgang.
- Skal privilegerede administrationsadgange kun udstedes på anmodning.
- Hvilke adgange skal evt. eksterne samarbejdspartnere have?

Det er blot nogle af de spørgsmål, der er gode at stille skarpt på, når du definerer adgangspolitikker.

Og mulighederne er mange. Start med at sætte politikker for dine mest kritiske apps og data først, og så arbejd dig ned igennem listen.



IDA går forrest i bekæmpelsen af it-kriminalitet

Som fagforening for ingeniører, naturvidenskabelige kandidater og it-professionelle, er det vigtigt at kunne sikre sine 110.000 medlemmers demokratiske ret til at holde deres medlemsskab fortroligt. Et samfundsansvar IDA - Ingeniørforeningen tager aktivt del i.

IDA har arbejdet målrettet med GDPR de seneste 4 år. Og det ændrede trusselsbillede har også givet IDA et nyt syn på it-sikkerhed. Fra en traditionel "udefra og ind" betragtning fokuserer IDA i dag i langt højere grad på; hvor ligger data, hvordan opbevarer vi data og hvordan transporterer vi data sikkert og krypteret hele vejen?

Video

Se video med IDA - Ingeniørforeningen om deres GDPR løsning.

timengo.
enter the cloud

57% af virksomheder har
yderst kritiske sårbarheder.

Mindre virksomheder er særligt udsatte,
da de har færre kompetencer på området
sammenlignet med større virksomheder.

timengo.
enter the cloud

10 gode råd...

...til den it-beredskabsplan du forhåbentlig aldrig får brug for

Trods de allerbedste intentioner, sikkerhedsstrategier, politikker og processer, vil der altid være en risiko for et angreb fra it-kriminelle. Derfor bør en beredskabsplan være en naturlig del af din samlede it-strategi.

Og du kan blive overrasket over, hvad der kan blive vigtigt under et angreb. Noget så banalt som søvn, hvem henter mad og hvem koordinerer kommunikationen internt og eksternt?

Derfor vil en "klokke-klar" plan komme dig til gode midt i en krisesituation og måske det værktøj, der begrænser tab, omkostninger og bringer forretningen på rette spor igen hurtigst muligt.

10 råd til din it-beredskabsplan

1. Tænk i roller og ansvar - ikke i scenarier. Du ved alligevel ikke, hvad du bliver ramt af.
2. En veldefineret it-beredskabsplanplan kommunikeret til organisationen. (Udprintet - dine systemer kan være nede).
3. Tydeligt defineret roller og ansvar, så ingen er i tvivl om deres opgave. (Udprintet - dine systemer kan være nede).
4. Udvælg et "IT War-room", så ingen er i tvivl om, hvor de skal møde op.
5. En "plan B" for hvor medarbejderne skal gå hen, hvis en lokation er nede, fx arbejde hjemme fra eller fra anden adresse i firmaet.
6. Udprintet telefonliste til brug for SMS-kommunikation, hvis angrebet sletter alt på telefonerne eller låser systemer.
7. Telefon bridge også en ekstern, hvis systemerne er nede. (Fx Skype privat, Webex, Intercall)
8. Pre-defineret og prioriteret applikation/systemliste over hvad der skal restores først, afklaret med forretningen. (Afklar kritikalitet og GDPR-problemer)
9. En proces for hvordan du løbende opdaterer planen.
10. Tag evt. udgangspunkt i vejledningen fra Nationalt Cyber Crime Center, hvis du ingen plan har i dag. **Find den her**.

Zero Trust

– i den virkelige verden

Studier fra Forrester viser, at
virksomheder som har indført en Zero Trust
tilgang oplever **50% færre sikkerhedsbrud** og
bruger 40% mindre tid på teknologi,
fordi det hele er integreret

Zero Trust er et mindset og ikke en "check-box" øvelse. Der er mange veje mod målet og ikke ét ideelt scenarie for opnåelse af Zero Trust - det afhænger af den enkelte virksomheds vision for it-sikkerhed.

Zero Trust er heller ikke et nyt begreb, men i takt med at cloud er blevet en større del af vores it-virkelighed, er modellens grundtanke blevet mere og mere aktuel for rigtig mange virksomheder. Hold dig for øje, at Zero Trust skaber forandringer og opgaver hos både brugere og administratorer – men tør vi undlade at gøre det?

Zero Trust integreret i Microsoft cloud

Hos timengo tænker vi Zero Trust ind som en integreret del af vores kunders Microsoft cloud.

Med udgangspunkt i Microsoft 365 hjælper vi virksomheder med at bygge sammenhængende it-sikkerhed på tværs af identiteter, enheder og data. Modellen for implementering kalder vi Cloud Platform. En leverancemodel der enkelt og effektivt aktiverer den tocifrede milliard investering, som Microsoft årligt bruger på udvikling af sikkerhedsteknologier.

Teknologier der samlet giver dig et komplet og solidt cyberforsvar og værktøjer til overholdelse af GDPR.

timengo.
enter the cloud

Zero Trust

– i den virkelige verden

Tag det første skridt mod Zero Trust
Du har nu forhåbentlig fået sat tankerne i gang omkring Zero Trust. Du kender grundprincipperne i modellen og hvad du skal overveje på din vej mod cloud ready it-sikkerhed.

Vil du høre mere om, hvordan timengo arbejder med Zero Trust og it-sikkerhed i Cloud er du altid velkommen til at kontakte os for en uforpligtende snak med en af vores cloud specialister, hvor vi kigger på, hvordan du kan implementere Zero Trust i din virksomhed.

Tak fordi du læste med. Med venlig hilsen Martin Lundsgaard, CTO i timengo.

For mere information om sikkerhed og Microsoft Cloud
besøg vores hjemmeside.
www.timengo.com