Today. Tomorrow. Together.

itm8®

GUIDE

10 solide **sikkerhedstips,** der straks styrker cyberforsvaret

Kære sikkerheds-ansvarlig!

Antallet af cyberangreb mod danske virksomheder stiger, og konsekvensen bliver stadig mere alvorlig for forretninger, der ikke er tilstrækkeligt beskyttet. Derfor er det afgørende at forholde sig til IT-sikkerheden – og evaluere løbende. For virkeligheden løber hurtigt fra et statisk beredskab.

Arbejd strategisk med sikkerheden
Stærk beskyttelse af din forretning kan du ikke opnå med genveje og lappeløsninger. Det kræver et fastlagt og vedholdende strategisk arbejde. Og ja, du bør lægge en strategi for, hvordan du gearer sikkerheden i din IT, så den matcher din forretning. Der er simpelthen for mange af dine forretningsprocesser, som er helt afhængige af IT-platformene til, at du har råd til at blive kompromitteret med lang nedetid til følge.

Kom i gang allerede i dag
Men det handler ikke kun om strategi. Der er også nogle basale tommelfingerregler, du kan følge, som omgående løfter din beskyttelse – og frigiver tid, til at du kan se på fremtidens forsvar.

Her er 10 ting, du kan implementere allerede i dag for at afvise hackerne og forsvare forretningen.

10 solide sikkerhedstips, der straks styrker cyberforsvaret

#01
Identificer hvilke af jeres systemer og udstyr, der er forretningskritiske

#02
Opnå ekstra gevinst ved stærke passwords

#03
Multifaktor log-in er den nye normal

#04
Opdater systemerne hele tiden

#05
Vedligehold adgange og rettigheder

#06
Sæt logs og alarmer op på det vigtigste udstyr

#07
Tag backup af det rigtige og verificer intervallerne

#08
Adskil adminstratorkonti fra brugerne med AD Tiering

#09
Luk adgangen til fjern-skrivebord via RDP

#10
Begræns muligheden for lokal administratoradgang

#01

Identificer hvilke af jeres systemer og udstyr, der er **forretningskritiske**

IT-platformene er blevet en del af stort set alle forretningsprocesser. Men der er nogen processer, der er mere afgørende for din forretnings fortsættelse end andre. Og de systemer skal have særlig opmærksomhed.

Du kan ikke beskytte noget, du ikke kender til. Derfor er det afgørende at få identificeret, hvilke af forretningens systemer, der støtter de vigtigste processer. Både så du kan beskytte såvel systemer og processer effektivt, men også så du kan evaluere, om du skal tage højde for redundans på nogle af de systemer – og eventuelt afvikle dem fra flere platforme samtidig for at sikre deres fortsættelse i tilfælde af et angreb på én af platformene.

Uanset hvad, handler det – i første omgang – ikke om teknik. Det handler om at forstå, hvilke processer der er vigtigst for forretningens fortsættelse, og derefter hvilke IT-systemer, er støtter dem, og som skal forsvares.

#02

Opnå ekstra gevinst ved **stærke passwords**

Stærke passwords gør det ikke alene. Men du kan lige så godt tage den ekstra gevinst, der ligger i at gå fra at kræve passwords på 8 eller 10 tegn til at kræve passwords på 14 tegn.

For den mængde tid, det tager at knække et password på 14 tegn, er i sig selv afskrækkende for hackere. De sidste fire karakterer fra 10 til 14 mangedobler antallet af variationer i passwordet og gør, at hackere går fra at skulle bruge en dag eller to på at knække koden til at skulle bruge måneder med de mest gængse metoder.

Oveni krav til passwordlængde kan du overveje at gøre mellemrum til et gyldigt tegn i passwords for at øge sikkerheden endnu mere. Og så er det måske værd at undervise ansatte i at bruge sætninger som passwords frem for kryptiske tegn-kombinationer eller enkelte ord.

Det er både mere sikkert og nemmere at huske, så det giver færre supportsager om reset af password.

#03

Multifator log-in er den nye normal

Du kender det allerede fra NemID og MitID – og du kan lige så godt lægge dig i slipstrømmen af de krav, som brugere kender fra de store offentlige IT-systemer og implementere de samme sikkerhedskrav i din forretning.

Multifaktor log-in (MFA) øger sikkerheden ved at se på tre områder: Hvad brugeren allerede ved (sit eget password), hvad brugeren allerede har (en sikkerhedstoken), og hvem brugeren er (en biometrisk godkendelse).

Tilsammen øger de tre faktorer sikkerheden, men de kan også hjælpe med at styre, hvem der har adgang til følsomme oplysninger, og hvorfra de er tilgængelige.

Den bedste løsning får du med en godkendelses-app, som for eksempel Microsoft Authenticator, men selv en løsning med SMS-godkendelse øger sikkerheden markant.

#04

Opdater systemerne hele tiden

Nyheden om en sårbarhed i et bredt benyttet system spreder sig som en steppebrand. For hackere giver det et tag-selv-bord af muligheder for at prøve sårbarheden af hos forskellige virksomheder og for at teste deres patch-niveau. Derfor handler det om at lukke hullerne ofte, så dine systemer ikke dukker op i toppen af listen med virksomheder, som hackerne vil afprøve.

For software er kun så sikker som den seneste opdatering. Og ofte er det først, når en svaghed begynder at blive udnyttet, at hullet bliver lukket. Derfor handler det om at være blandt de første til at patche systemerne, så sårbarheder og svagheder bliver adresseret, inden hackere når frem til at prøve dem af på netop jeres systemer.

Det handler ikke altid om at være bedre end hackerne, nogle gange er det rigeligt at være bedre beskyttet end konkurrenterne, hvis du vil undgå uønsket opmærksomhed fra IT-kriminelle.

#05

Vedligehold adgange og rettigheder

Når en ansat i din virksomhed stopper, følger der en hel del digital oprydning med. Både for at holde orden på jeres data, men helt klart også for at øge sikkerheden. For i mange tilfælde tager brugere også virksomhedsdata med sig – ikke nødvendigvis af ond vilje, men fordi adgangen til data fortsætter efter ansættelsen ophører.

Men opgaverne stopper ikke sammen med dine ansatte. For de aktive brugere skifter også gerne privelegier og rettigheder løbende – men hvem forholder sig til, om det er nødvendigt? Eller til om en rettighed, der bliver givet midlertidigt, nu også rulles tilbage igen?

Forældede og forkert indstillede brugerkonti giver hackere en større angrebsflade og giver mulighed for, at brugerne kan blive en genvej for kriminelle til at skaffe sig bredere og dybere adgang til jeres systemer.

Derfor skal I have en procedure for opdatering og vedligehold af brugeradgangen, inklusiv en proces for at deaktivere og slette brugere, der forlader virksomheden.

45% fortæller, at deres virksomhed har været **udsat for mindst én sikkerhedshændelse** i løbet af de seneste 12 måneder.[1]

1: PwC's Cybercrime Survey 2023

#06

Sæt **logs og alarmer** op på det vigtigste udstyr

Hvis du er under angreb, opdager du det så overhovedet? Eller kan en hacker gemme sig i systemerne i månedsvis og vente på en oplagt lejlighed til at udnytte sin position?

Du er nødt til at holde øje med, hvad der sker i de vigtige systemer, så du kan spotte, når noget ikke er, som det plejer at være. Du skal for opdage, når en bruger for eksempel forbinder til virksomhedens systemer fra en uventet placering. Hastighed spiller en stor rolle, hvis et system er kompromitteret.

Derfor skal du have en alarm, når et centralt system opfører sig unormalt, så du kan agere hurtigt.

Og når du skal finde ud af, hvad der faktisk er sket i et system, er gode logs din bedste ven. Uden gode logs skyder du i blinde efter løsninger på de sikkerhedsbrud, du kan være blevet udsat for.

#07

Tag backup af det rigtige og verificer intervallerne

Din backup er ligegyldig, hvis den ikke indeholder alt det forventede data, eller hvis den ikke kan gendannes. Din virksomhed får løbende ny data, og du skal med sikkerhed kunne sige, om de nye data er med i din backup-plan.

For eksempel er det vigtigt, at du ved implementering af et nyt økonomisystem (ERP-system) får verificeret, om det nye system også indgår i din backup. Desuden bør muligheden for gendannelse også regelmæssigt kontrolleres, så du kan være sikker på, at din backup rent faktisk virker, hvis ulykken rammer.

Din backup redder dig ikke, hvis den rammes af den samme katastrofe, som rammer selve serveren med dine data. Derfor bør din backup placeres væk fra din lokation, så den er i sikkerhed mod brand, tyveri mm. Her kan du med fordel følge 3-2-1-reglen: Hav altid tre kopier af din backup, fordelt på to forskellige medier og opbevar en af kopierne på en anden lokation.

#08

Adskil administrator-konti fra brugerne med AD Tiering

Adgangskontrol er en vigtig del af dit digitale forsvar. Og det er særligt vigtigt at afgrænse brugere med særlige privilegier fra almindelige slutbrugere. En hacker vil nemlig ofte prøve at knække adgangen til en almindelig brugers konto, og så bruge den adgang til at bevæge sig horisontalt i dine systemer for at kompromittere en bruger med flere rettigheder.

Dit Active Directory spiller en central rolle i det forsvar - og derfor skal du dele AD identiteter og systemer op i kategorier. Typisk arbejder man med Tier 0, Tier 1 og Tier 2 - og brugere skal placeres i den kategori, der passer med deres adgangsbehov. På den måde kan du begrænse sandsynligheden for, at en kompromitteret brugerkonto kan bruges til at få adgang til en konto med højere adgangsniveau.

#09

Luk adgangen til fjernskrivebord via RDP

Under optimale - og kontrollerede forhold - kan remote desktop adgang være en god idé på dit interne netværk. Men RDP kræver moden IT-sikkerhed for at kunne lukke af for hijacking, uvedkommende adgange og sessioner, exploits og eskalering af privilegier.

Hvis din remote desktop adgang ikke bliver håndteret stringent og korrekt, betyder det nærmest per definition, at du udsætter din forretning for en uacceptabel sikkerhedsrisiko. Og RDP-adgang via internettet er i alle tilfælde helt udelukket, hvis du vil øge sikkerheden.

Hvis du tillader RDP, men ikke ved med sikkerhed, hvordan adgangen er sikret, skal du tjekke det med det samme. Og selvom du bruger RDP med åbne øjne og har gjort noget for at sikre adgangen, skal du overveje, om din sikkerhed kan leve med den eksponering, der følger med, eller om du helt skal aflive muligheden og finde andre og mere sikre løsninger.

Det kunne være en Citrix-løsning eller muligheden for at indføre særlige 'Priveleged Access Workstations', der som de eneste har ret til at forbinde via RDP, så du får langt større kontrol med sikkerheden.

#10

Begræns muligheden for **lokal administratoradgang**

Skal man tro sikkerhedsfirmaet BeyondTrusts Microsoft Vulnerabilitites rapport fra 2022, så kunne 75% af alle sårbarheder fra 2015 til 2020 være undgået, hvis brugeren ikke havde haft lokale administratorrettigheder på deres arbejdscomputer.

Brugerne er en af de største sårbarheder i dit digitale forsvar, så hvorfor får de lov til frit at installere apps på deres arbejdscomputer, som de har fundet på skumle hjemmesider. Det gør de heller ikke, hvis du tager sikkerheden alvorligt.

Filer og programmer fundet online er en genvej til at introducere malware og sikkerhedstrusler på virksomhedens netværk. Den genvej skal du lukke. For det holder malware væk fra virksomhedens arbejdsstationer. Det bevarer det forsvar, du allerede har sat op. Det sørger for, at virksomhedens maskiner lever op til de centrale krav, der er opsat. Og det beskytter resten af din organisation mod hackere.

Har du **spørgsmål?**

Snak med vores IT-specialister. Vi er altid klar til at rådgive dig om, hvordan du kan beskytte din forretning endnu bedre.

Johnni Meldgård Rude
Security Director

+45 3132 9006
jorud@itm8.com

Today. Tomorrow. Together.

itm8®

Lad os bygge fremtidens IT. **Sammen.**

Kontakt os i dag.

+45 6916 0004

information@itm8.com

www.itm8.dk