Ransomware-ready?
Praktische tips voor fundamentele maatregelen

Een effectieve beveiliging tegen ransomware is geen lappendeken van losse maatregelen maar een continue proces dat door de hele organisatie heen loopt. Met deze tien maatregelen legt u hiervoor het fundament.

Risicoanalyse Risicoanalyse

Cybersecurity draait om het beschermen van de bedrijfskritische systemen en data. Bij een onderwijsinstelling zijn dat bijvoorbeeld de gegevens van studenten. Een retailer wil voorkomen dat de kassa- en voorraadsystemen door ransomware worden platgelegd. Deze 'kroonjuwelen' identificeren uw assetanalyse. Ook brengt u de voornaamste bedreigingen in kaart, vervolgens bepaalt u impact voor bedrijfscontinuiteit wanneer er X of Y met asset A of B gebeurt (business impact analyse).

Patches en hardening

Hanteer voor alle hardware en software een strikt patch- en updatebeleid, zodat cruciale beveiligingsupdates zo snel mogelijk geïnstalleerd worden. Zorg er verder voor dat alle systemen veilig geconfigureerd zijn en schakel overbodige functies uit. Dit wordt hardening genoemd. Ook is het belangrijk dat u een goed overzicht heeft van alle IT-systemen. Dan kunt u sneller handelen als er een nieuwe kwetsbaarheid wordt ontdekt.

Toegangsbeheer

Beperk de toegang tot systemen en data, zodat deze afgeschermd zijn van de buitenwereld. Het uitgangspunt van Identity & Access Management (IAM) is: hoe minder toegang, hoe beter. Een werknemer krijgt alleen toegangsrechten die nodig zijn voor werk. Wees extra voorzichtig met het toekennen van beheerdersrechten. Deze accounts zijn zeer interessant voor cybercriminelen en moeten dus ook goed gemonitord worden.

Logging en detectie

Monitoring vormt de basis van de beveiliging. Door logbestanden van bedrijfssystemen bij te houden en afwijkingen te signaleren, kan een ransomware-aanval in een vroegtijdig stadium worden gedetecteerd. Ook maakt logging het makkelijker om te begrijpen hoe een incident kon plaatsvinden en wanneer het is begonnen.

Multifactor-authenticatie

Wachtwoorden zijn inherent onveilig. Ze kunnen onder andere via phishing gestolen worden of op een andere manier op internet belanden. Multifactorauthenticatie (MFA) voorkomt dat een aanvaller kan inloggen met alleen een gebruikersnaam en wachtwoord. De gebruiker moet zijn identiteit ook op een andere manier aantonen, bijvoorbeeld met een sms-code. Het activeren van MFA gaat ongeoorloofde toegang tot bedrijfssystemen tegen.

Macro's uitschakelen

Macro's automatiseren bepaalde taken in kantoorsoftware, maar ze worden ook gebruikt voor het verspreiden van malware. Een veelgebruikte truc is het versturen van een nepfactuur. De gebruiker moet de macro's activeren om de factuur te bekijken, waarna de malware wordt gedownload. IT-beheerders dekken dit risico bijvoorbeeld af door alle macro's standaard uit te schakelen zonder dat de gebruiker dit kan herstellen.

Endpoint-beveiliging

Malware komt vaak binnen via malafide bijlages en het onbewust downloaden van bestanden (drive-by downloads). Een extra beveiligingslaag op endpoints zoals laptops en smartphones helpt dit te voorkomen. Een moderne oplossing voor endpointsecurity detecteert zowel bekende als nieuwe malware. Ook stelt u met zo'n oplossing in welke applicaties veilig zijn om te gebruiken. Schadelijke software wordt geblokkeerd.

Back-ups

Misschien wel de belangrijkste maatregel is het maken van meerdere back-ups. Zorg dat u minstens drie kopieën van bedrijfskritische data heeft op verschillende opslagmedia, zoals een externe harde schijf of op tape. Verplaats minstens één back-up naar een andere fysieke locatie of naar de cloud, en zorg voor minstens één offline back-up. Dit wordt de 3-2-1-1-regel genoemd. Test de back-ups ook regelmatig op verschillende manieren. Een recente back-up is essentieel in het geval van een ransomware-aanval.

Netwerk-segmentatie

De aanvallers proberen zoveel mogelijk systemen te besmetten voordat ze de ransomware activeren. Daarom is het belangrijk om het netwerk goed te segmenteren. Dit betekent dat het netwerk in meerdere zones wordt verdeeld. Dat doet u bijvoorbeeld met behulp van firewalls. Door deze digitale branddeuren wordt het moeilijker om het gehele netwerk te compromitteren.

Incident-responseplan

Ga ervan uit dat uw bedrijf ooit slachtoffer wordt van ransomware. Belangrijke systemen zijn niet beschikbaar, uw bedrijfsvoering raakt ontregeld en de cybercriminelen eisen een fors geldbedrag. Hoe handelt u dan? Wat is uw beleid ten aanzien van het losgeld? Hoe ziet de herstelprocedure eruit? Hoe communiceert u met klanten en de media? Leg dit vast in een plan en oefen de afspraken regelmatig met verschillende afdelingen.