Ransomware Protection Checklist

Aanvallers gebruiken steeds geraffineerdere ransomware en weten de bestaande verdedigingsmechanismen steeds beter te omzeilen. Gebruik deze checklist om de aanvaller en de ransomware te slim af te zijn.

1. Bescherm uw e-mail

Ransomware-aanvallen beginnen vaak met een phishing-e-mail om inloggegevens van beheerders of gebruikers te achterhalen.

1a	**Blokkeer phishing-aanvallen** Aanvallers gebruiken social engineering om de traditionele e-mailbeveiliging te omzeilen. Gebruik een oplossing voor e-mailbeveiliging met AI-bescherming tegen phishing en accountovernames met waarschuwingen wanneer schadelijke activiteiten worden gedetecteerd.	☐
1b	**Train medewerkers** Je gebruikers zijn de laatste verdedigingslinie van je organisatie tegen phishing-aanvallen. Er moet voortdurend training worden gegeven, omdat de aanvallen in de loop der tijd vaak geraffineerder worden.	☐
1c	**Voer herstel uit** Aanvallen die de e-mailbeveiliging omzeilen en in de inbox van gebruikers terechtkomen, moeten snel worden aangepakt. Kies een oplossing voor e-mailbeveiliging die bedreigingen proactief opspoort en herstel automatiseert.	☐

2. Beveilig uw applicaties.

Aanvallers kunnen je webapplicaties hacken om toegang te krijgen tot je gegevens.

2a	**Bescherm webapplicaties** Toepassingen hebben vaak kwetsbaarheden die kunnen worden misbruikt om toegang tot je gegevens te krijgen. Gebruik een oplossing voor de beveiliging van toepassingen die bescherming biedt tegen kwetsbaarheden van webapplicaties, zoals de OWASP Top 10, zero-day attacks en brute force attacks.	☐
2b	**Bescherm de toegang tot applicaties** Voor interne applicaties is het aanbevolen om alleen toegang te verlenen aan geautoriseerde gebruikers en apparaten. Kies voor een zero-trust oplossing met toegang op basis van rollen, multifactorauthenticatie en voortdurende verificatie van de identiteit van gebruikers en apparaten..	☐
2c	**Voorkom lateral movement op uw netwerk** Als aanvallers toegang krijgen tot je netwerk, proberen zij vaak via lateral movement gegevensbronnen te vinden en te infecteren. Je hebt een netwerkfirewall nodig die zowel je lokale netwerk als je cloudnetwerk beschermt met netwerksegmentatie en geavanceerde beveiligingsdiensten.	☐

3. Maak een back-up van je gegevens.

Aanvallers versleutelen je gegevens en eisen losgeld.

3a	**Maak een back-up van je gegevens** Je moet een back-up maken van al je gegevens. Denk zowel aan je lokale gegevens als aan de gegevens in cloud/SAAS-toepassingen, zoals Office 365.	☐
3b	**Bescherm de toegang tot applicaties** Aanvallers hebben het vaak op je back-ups gemunt om te voorkomen dat jij je gegevens kunt herstellen. Versleuteling, toegangscontrole en IP-beperkingen zijn daarbij allemaal van belang. Je moet ervoor zorgen dat de toegang tot jouw gegevens eenvoudig is voor jou, maar moeilijk voor aanvallers.	☐
3c	**Stel een herstelplan op** Als je wordt aangevallen, moet je de aanval snel kunnen afslaan, jouw gegevens kunnen herstellen en voorkomen dat je losgeld moet betalen. Denk niet alleen aan je technische reactie, maar ook aan je zakelijke reactie. Test je volledige plan voordat er zich problemen voordoen. Forensisch onderzoek kan van pas komen in de nasleep van een aanval om kwetsbaarheden te vinden.	☐

Andere aanbevelingen

- **Patching** – Zorg ervoor dat software is gepatcht en bijgewerkt. Aanvallers zoeken eerst naar bekende kwetsbaarheden, dus maak het ze niet te gemakkelijk.
- **Password Security** – Zorg voor sterke wachtwoorden. Veel van de recente aanvallen zijn geslaagd dankzij zwakke wachtwoorden en inefficiënt wachtwoordbeheer.
- **Multifactorauthenticatie** – Overweeg om voor alle toepassingen en middelen een tweefactorauthenticatie via telefoon of sms verplicht te stellen. Op deze manier kun je brute-force inlogpogingen voorkomen

Wil je ook aan de slag met jouw security?
Lees dan meer over al onze oplossingen in onze security whitepaper

Klik hier!

Patrich Voss
Solution advisor security
T +31 40 760 2915
patrick.voss@bechtle.com