

# RANSOMWARE: PREVENTIE EN BEVEILIGING

## REALTIME BEVEILIGING

Ransomware vormt in toenemende mate een bedreiging. Het is een vorm van malware waarbij kwaadwillenden computersystemen blokkeren en die blokkering pas opheffen na ontvangst van een geldbedrag. Andere malware blijft vaak lange tijd verborgen tot het in werking treedt, maar ransomware is zo ontworpen dat het snel werkt. Verspreiding van deze vorm van malware gebeurt via spear phishing, valse websites en corrupte downloads. Financiële instellingen zijn bijzonder gevoelig voor de impact van ransomware, enerzijds omdat het een bedreiging vormt voor de capaciteit om bedragen snel en efficiënt over te boeken, en anderzijds omdat ze worden beschouwd als lucratieve doelwitten. Kwaadwillenden houden zich niet altijd aan hun belofte; zelfs na het betalen van losgeld weigeren sommige aanvallers de malware te verwijderen of vertrouwelijke gegevens vrij te geven.

- Investeer in systemen voor malwarebeveiliging die zich in realtime aanpassen aan nieuwe, intelligentere bedreigingen.
- Evalueer de veiligheid van alle met een netwerk verbonden apparaten waarop gevoelige of essentiële informatie is opgeslagen. Verbind alle niet-noodzakelijke systemen met een apart netwerk.
  - Wees vooral voorzichtig met IoT- of "smart-apparaten" op de werkplek. Deze apparaten beschikken vaak over zwakkere of zelfs geen beveiligingssystemen en kunnen als doelwit worden gebruikt voor toegang tot essentiële systemen.
  - Houd rekening met de beveiliging van systemen voor werken van huis. Zorg dat beveiligingstools ook het internetverkeer van buiten het bedrijfsnetwerk kunnen bewaken.
- Geef voorlichting aan werknemers over phishingaanvallen en de noodzaak om sterke wachtwoorden te gebruiken.
- Overweeg de implementatie van multifactorverificatie in de hele organisatie, voor zover mogelijk.
- Zorg dat alle software en systemen regelmatig worden bijgewerkt. Configureer de instellingen indien mogelijk zodat updates automatisch worden uitgevoerd.
- Stel een plan op voor incidenten- en crisisbeheer, zodat duidelijk is hoe moet worden gereageerd op een aanval door ransomware en het verlies van waardevolle gegevens.
  - Bepaal een extern communicatieplan voor het geval van een aanval door ransomware.

## GEGEVENSBACK-UPS

- Investeer in veilige, regelmatig bijgewerkte back-upsystemen om uw gegevens te beschermen.
  - Zorg dat USB-apparaten en externe harde schijven na voltooiing van back-ups fysiek worden losgekoppeld van met het netwerk verbonden computers.
  - Voorzie servers van hoogwaardige versleuteling en verificatie in meerdere stappen als u gebruikmaakt van opslag in de cloud.
- Maak een alleen-lezen kopie van de hoofddirectory voor herstel na een rampsценario.
- Ontwikkel systemen die geautomatiseerd gegevensherstel uitvoeren.
- Ontwikkel scenario's om te bepalen hoelang het zal duren om cruciale gegevens en bedrijfservices te herstellen.

## REGELGEVING

- Controleer wat de relevante lokale juridische richtlijnen zijn voor ransomware.
  - Houd rekening met landspecifieke richtlijnen. Ontwikkel een plan voor periodieke evaluatie van gewijzigde richtlijnen.
  - Houd rekening met specifieke richtlijnen voor de financiële sector.
  - Houd rekening met internationale juridische en wettelijke vereisten.
- Beoordeel wat de risico's zijn met betrekking tot het betalen van losgeld. In sommige gevallen kunt u zich door het betalen van losgeld schuldig maken aan de schending van bestaande maatregelen tegen kwaadwillenden.
- Werk samen met de plaatselijke politie. Bouw relaties op, zodat u in het geval van een aanval snel informatie kunt uitwisselen.
- Beoordeel wat de voor- en nadelen zijn van cyberbeveiligingsbeleid met betrekking tot ransomware.

## Inschatten in hoeverre uw organisatie is voorbereid op ransomware

Stel de volgende vragen bij het opstellen van een plan voor preventie en bescherming tegen ransomware.

1. Heeft uw organisatie een **schema voor regelmatige back-ups**?
  - Worden deze back-ups los van uw netwerk uitgevoerd, namelijk via cloudopslag of fysiek geïsoleerde USB-apparaten of externe harde schijven?
2. Zijn er **niet-essentiële apparaten** die verbinding maken met het netwerk van uw organisatie?
  - Kunnen deze worden verplaatst naar andere netwerken die geen gevoelige gegevens bevatten?
3. Begrijpt uw organisatie wat de **wettelijke en juridische risico's** zijn van het betalen van losgeld?
  - Wettelijke richtlijnen variëren per land en worden regelmatig gewijzigd.
4. Worden de software en systemen van uw organisatie regelmatig bijgewerkt? Worden deze updates **automatisch** uitgevoerd?
5. Beschikt uw organisatie over een **plan om te reageren op een aanval door ransomware** en om te gaan met verlies van waardevolle gegevens?
6. Beschikt uw systeem over een **cyberbeveiligingsbeleid**? Zo ja, op welke manier houdt dit plan rekening met aanvallen door ransomware?
  - In sommige plannen is een verbod op het betalen van losgeld opgenomen, volgens ander beleidslijnen moet juist wel worden overgegaan tot betaling als onderdeel van het beleid.