CYBERBEVEILIGING VOOR KLEINERE ORGANISATIES

CHECKLIST RANSOMWARE

PARAATHEID VOOR RANSOMWARE

☐ **Zorg dat u bij de ontwikkeling van een preventie- en beschermingsplan voor ransomware regelmatig het evalueert:**

- Heeft uw organisatie een schema voor regelmatige back-ups?
- Zijn er niet-essentiële apparaten die verbinding maken met het netwerk van uw organisatie?
- Begrijpt uw organisatie wat de wettelijke en juridische risico's zijn van het betalen van losgeld?
- Worden de softwaresystemen van uw organisatie regelmatig bijgewerkt? Worden deze updates automatisch uitgevoerd?
- Beschikt uw organisatie over een plan om te reageren op een aanval door ransomware en om te gaan met gegevensverlies?
- Beschikt uw systeem over een cyberbeveiligingsbeleid? Zo ja, op welke manier houdt dit plan rekening met aanvallen door ransomware?

REALTIME BEVEILIGING

☐ **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.
- ☐ 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 rampscenario.**

☐ **Ontwikkel systemen die geautomatiseerd gegevensherstel uitvoeren.**

☐ **Ontwikkel scenario's om te bepalen hoelang het zal duren om cruciale gegevens en bedrijfsservices te herstellen.**

REGELGEVINGSKLIMAAT

- ☐ **Controleer wat de relevante lokale juridische richtlijnen zijn voor ransomware.**
  - ☐ Houd rekening met landspecifieke richtlijnen.
  - ☐ Houd rekening met specifieke richtlijnen voor de financiële sector.
  - ☐ Houd rekening met internationale juridische en wettelijke vereisten.
  - ☐ Ontwikkel een plan voor periodieke evaluatie van gewijzigde richtlijnen.
- ☐ Beoordeel wat de risico's zijn met betrekking tot het betalen van losgeld.
- ☐ 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.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

CarnegieEndowment.org

THE WORLD BANK IBRD • IDA | WORLD BANK GROUP
SWIFT INSTITUTE
FS-ISAC
Standard Chartered
CYBER READINESS INSTITUTE
GLOBAL CYBER ALLIANCE
ICBA Independent Community Bankers of America®