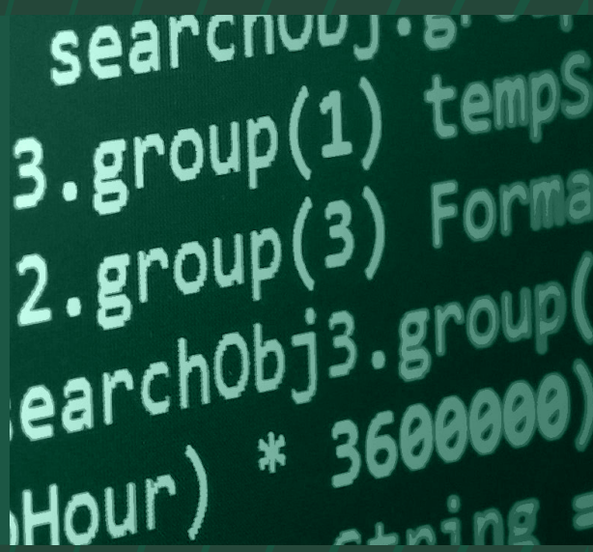
DELL Technologies

5 Aanbevelingen voor het doorstaan van een ransomware-aanval



1 Houd een uitgebreid actieplan bij incidenten in stand

Richt u op het minimaliseren van de impact van een aanval

Oefen, test en update vaak

Zorg dat er van tevoren een incidentresponsteam klaarstaat

Overweeg cyberverzekering als onderdeel van uw algehele tolerantiestrategie

Neem plannen op om samen te werken met wetshandhaving

2 Zorg voor een duidelijke communicatiestrategie

Maak van tevoren communicatiesjablonen

Zorg voor tijdige en duidelijke communicatie binnen de organisatie

Wees bereid om extern te communiceren, indien van toepassing

Houd u aan de toepasselijke meldingsvoorschriften

3 Zorg voor robuuste databescherming

Bescherm kritieke data in een geïsoleerde, onveranderbare, air-gapped datakluis

Geef prioriteit aan herstel per service/infrastructuur

Oefen regelmatig op herstelbaarheid

Koppel mogelijkheden zoals cleanroom aan uw beoogde hersteltijd

Garandeer de integriteit van herstelbare data

4 Ga niet uit van een onmiddellijke terugkeer naar de normaliteit

Het betalen van losgeld moet een laatste redmiddel zijn

Zorg ervoor dat u voldoet aan wet- en regelgeving voordat u betaalt

Er is geen garantie dat de hacker uw data zal teruggeven, zelfs niet als er losgeld wordt betaald

5 Leg de nadruk op training en opleiding

Voer aanvalsimulaties uit

Monitor en test de gewoontes van werknemers op het gebied van cyberhygiëne

Maak gebruik van tools zoals phishingtests en training in e-mailbeveiliging

Het is niet langer een kwestie van 'of', maar 'wanneer'.

Ondernemingen moeten plannen alsof een aanval onvermijdelijk is, ondanks hun beste verdedigingen. Om te bespreken wat te doen als het noodlot toeslaat, spraken Dell Subject Matter Experts Jim Shook, Global Director of Cybersecurity and Compliance Practice, en Steven Granat, Principal Consultant, Cybersecurity Solutions and Strategic Partnerships, met Brian White, Senior Consultant, Product Marketing bij Dell Data Protection.

> U moet de juiste mensen erbij betrekken, een oefening uitvoeren en acties simuleren, zodat iedereen meteen weet wat te doen als er een aanval plaatsvindt."
>
> ***Steven Granat**, Principal Consultant, Cybersecurity Solutions and Strategic Partnerships, Dell Technologies*

Houd een uitgebreid actieplan bij incidenten in stand

Wanneer een aanval plaatsvindt, moeten alle belangrijke belanghebbenden – vrijwel iedereen binnen de organisatie en ook derden zoals leveranciers – weten wat ze moeten doen. Een schriftelijk actieplan bij incidenten moet een duidelijke volgorde van acties schetsen, adviseert Shook. Een uitgebreid plan behandelt technologische, proces- en communicatiestappen, van onmiddellijke actie tot en met herstel. Zorg ervoor dat u ook een papieren versie van het plan bijhoudt, aangezien digitale communicatiemiddelen mogelijk niet operationeel zijn. "U hebt een plan nodig dat u letterlijk van de plank kunt pakken", zegt Granat.

Zorg voor een duidelijke communicatiestrategie

De meeste organisaties zullen moeten communiceren met de belangrijke belanghebbenden en moeten in veel gevallen voldoen aan wettelijke vereisten. Maak verschillende sjablonen voor zowel interne als externe communicatie met systematische instructies voor wie in welke volgorde en wanneer op de hoogte moet worden gesteld. Houd er rekening mee dat telefoon- en e-mailsystemen mogelijk niet werken.

Implementeer een robuuste databeschermingsstrategie

Een belangrijk doel bij het doorstaan van een ransomware-aanval is om de data zo pijnloos mogelijk te herstellen, terwijl het betalen van losgeld wordt vermeden. Een sterke databeschermingsstrategie is een belangrijk onderdeel van het bereiken van deze doelstellingen, maar zal zowel technologie als processen moeten omvatten. "Gebruik onveranderbare data en cyberkluizen om voldoende data op te slaan die u kunt vertrouwen, of tenminste als validatiepunten om systemen te kunnen herstellen", adviseert Shook. Ervoor zorgen dat de data worden beschermd, is de eerste stap; daarnaast moet u de juiste mensen en processen hebben om deze te kunnen herstellen. Externe deskundigen kunnen hierbij helpen, maar zij moeten in de planningsfase worden ingeschakeld.

Ga niet uit van een onmiddellijke terugkeer naar de normaliteit, zelfs niet als u losgeld betaalt

Het betalen van losgeld, wat alleen als laatste redmiddel mag worden beschouwd, garandeert niet dat alles direct weer functioneert. Vergeet niet dat u onderhandelt met een crimineel, en zelfs als u de decoderingssleutels krijgt, heeft u een strategie nodig voor de nieuw herstelde data. Om te beginnen moet u de gedecodeerde data testen en alle systemen methodisch opnieuw opbouwen. Het herhalen van nauwgezette aandacht voor wat-als-gebeurtenissen voordat er zelfs maar een aanval plaatsvindt, zal een grote bijdrage leveren aan het bereiken van tolerantie. "Inzicht in de verschillende applicaties en afhankelijkheden in uw technische infrastructuur is van cruciaal belang voor een efficiënte terugkeer naar een stabiele toestand. 'Heb ik een bruikbare herstelbron en een herstelbaar doel?' 'Heb ik data die niet gecompromitteerd zijn?' Dit zijn belangrijke overwegingen om over na te denken", zegt Granat.

In de herstelfase moet u er ook zeker van zijn dat de aanvaller uw systemen daadwerkelijk heeft verlaten. "U moet ervoor zorgen dat de brand in uw huis geblust is en ook uitzoeken waardoor die brand in de eerste plaats is ontstaan, want zonder deze twee cruciale informatiepunten stelt u zich bloot aan toekomstige aanvallen", zegt Shook.

Training en oefening zijn van cruciaal belang

Een belangrijk onderdeel van cybertolerantie is uitgebreide training, die varieert van ervoor zorgen dat werknemers een goede cyberbeveiligingshygiëne toepassen tot het routinematig oefenen van het herstelplan. "U moet de juiste mensen erbij betrekken, een oefening uitvoeren en acties simuleren, zodat iedereen meteen weet wat te doen als er een aanval plaatsvindt" zegt Shook.

Ransomware is wellicht onvermijdelijk in het huidige dreigingslandschap, maar door middel van planning en uitvoering kunt u de operationele, financiële en reputatie-impact minimaliseren. Het doel is om zo snel en pijnloos mogelijk terug te keren naar normaal.

Ontdek hoe u enkele van de grootste uitdagingen op het gebied van cyberbeveiliging van vandaag kunt aanpakken op **dell.com/cybersecuritymonth**