Emergency Response Toolkit:

HOE REAGEREN OP EEN RANSOMWARE AANVAL IN 12 STAPPEN

Organisaties moeten ervan uitgaan dat zij vroeg of laat met een ransomware aanval te maken krijgen. De belangrijkste vraag is wanneer. Voorbereiding is de sleutel.

Dit is een gids met acties voor bedrijven die het slachtoffer zijn van een ransomware aanval.

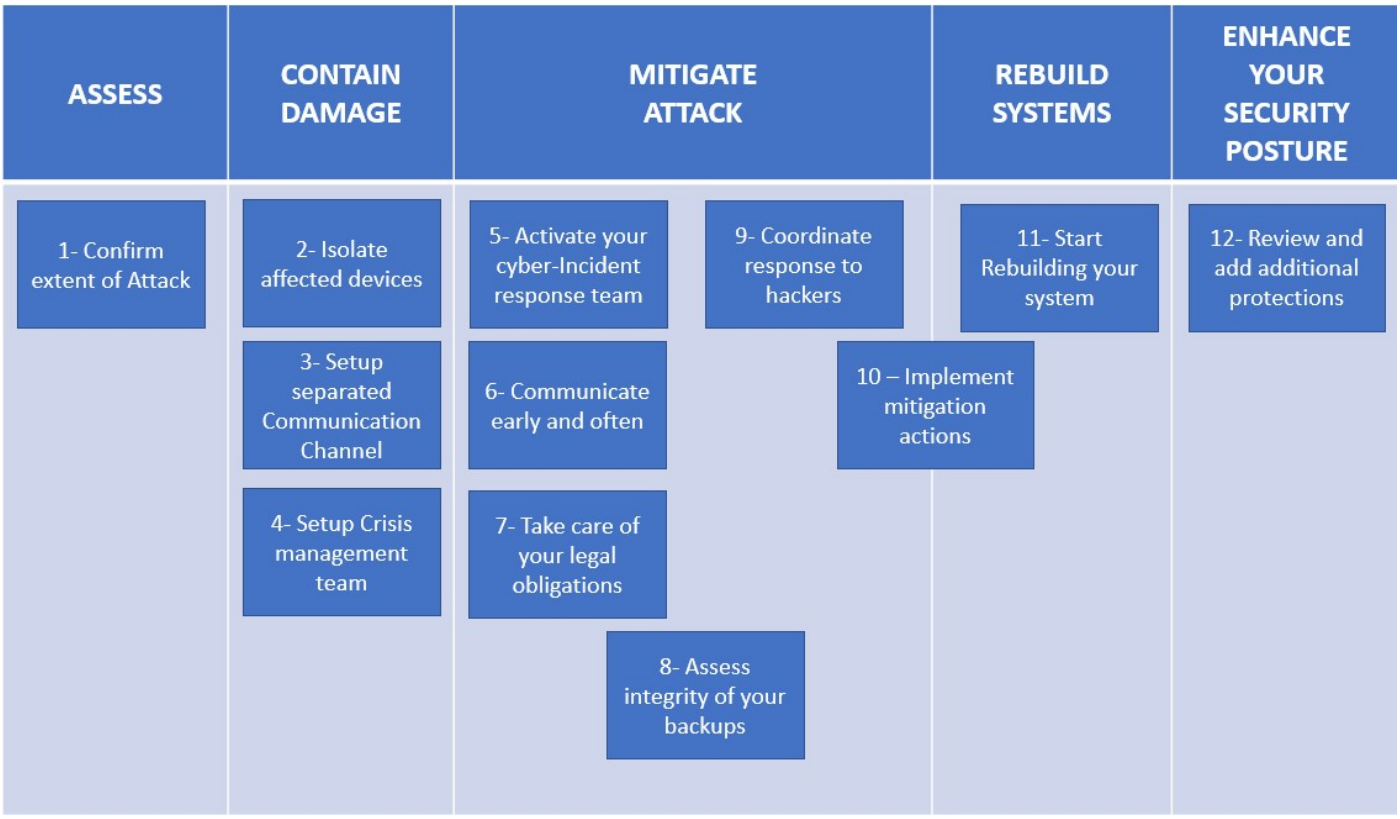
Voorbereiding is essentieel bij het aanpakken van een ransomware aanval. Het primaire doel is ervoor te zorgen dat organisaties voorbereid zijn en niet hoeven te improviseren zodra een ramp toeslaat, wat tot extra fouten zal leiden die kunnen resulteren in het verlies van nog meer gegevens.

Voorbereiding houdt in dat u zeker weet welke teams u nodig hebt (technisch, crisis, communicatie, ...) en hoe deze mensen snel te bereiken. Terwijl u zich voorbereidt (d.w.z. uw draaiboek is beschikbaar, u hebt het getest met een oefening), moet u ervoor zorgen dat dit ook een proces omvat om alles up-to-date te houden.

De onderstaande stappen zijn de minimumstappen die u moet volgen in geval van een ransomware-aanval, hopelijk door uw noodherstelplannen toe te passen, zo niet hopen wij dat de onderstaande richtlijnen de belangrijke actiepunten zullen belichten.

Herstellen van een ransomware aanval is niet in een paar uur geklaard en zal weken of maanden duren. Maatregelen in de uren na een bevestigde aanval zijn echter cruciaal.

Visuele stappen op 'high level'



1. Bepalen en bevestigen van de omvang van de ransomware aanval

De systemen opnieuw opbouwen, is NIET de eerste stap in uw reactieplan.

Beoordeel de omvang van de ransomware aanval door te kijken naar wat is versleuteld en/of mogelijk is geëxfiltreerd. Een antwoord op deze vraag is van cruciaal belang voor het activeren van een responsplan.

Dit responsplan verschaft nuttige inzichten in de interne en externe vragen van het management, werknemers en klanten.

Het opstellen van een responsplan is moeilijk als je de omvang van de aanval niet kent. Probeer te documenteren welke gegevens op de versleutelde machines stonden en zoek naar gegevens die mogelijk zijn geëxfiltreerd.

2. Isoleer geïnfecteerde apparaten

Isoleer geïnfecteerde apparaten zo veel mogelijk om verdere verspreiding te voorkomen.

Wanneer ransomware toeslaat, is het essentieel om getroffen apparaten zo veel mogelijk te isoleren om verdere verspreiding te voorkomen. Ga ervan uit dat aanvallers al goed zijn ingebed in uw omgeving tegen de tijd dat de ransomware aanval wordt uitgevoerd, dus snel handelen om de gevolgen te beperken is essentieel.

Begin met het isoleren van de geïnfecteerde apparaten en verwijder ze van het netwerk. Sluit netwerkkabels af, stop netwerkverbindingen (ook WiFi-netwerken).

Als uw netwerk het toelaat en goed gesegmenteerd is, kunt u ook het geïnfecteerde netwerksegment loskoppelen.

Zet de geïnfecteerde apparaten NIET UIT, voorkom dat systemen worden afgesloten. Er kan nog steeds malware geïnstalleerd zijn die niet geactiveerd is. Het hebben van een werkend systeem kan ook helpen bij het inroepen van hulp van een incident response bedrijf om gedetailleerd onderzoek te doen.

Begin niet met herstelwerkzaamheden zolang de omvang van de aanval niet duidelijk is, dit omvat de methode, het tijdstip, de getroffen systemen.

3. Zet een gescheiden communicatiekanaal op

Ga ervan uit dat uw bedrijfscommunicatiemiddelen (indien nog functioneel) gecompromitteerd zijn.

Gevoelige communicatie over de evolutie van het incident gebeurt via een gescheiden en beveiligd kanaal. Ga ervan uit dat uw mailsystemen (indien nog functioneel) ook geïmpacteerd zijn en dat de aanvaller daar toegang toe heeft, wat betekent dat de communicatie op uw netwerk tot het strikte minimum moet worden beperkt. Analyseer welke systemen gebruikt kunnen worden om intern en extern te communiceren. Zet een beveiligd communicatiekanaal op met uw technische team, leiderschapsteam.

Het opzetten van bv. Signal of tijdelijk gebruik van een extern conferencingsysteem (Secure communication tool) en het creëren van gescheiden groepen is aan te bevelen. Misschien wilt u een groep opzetten met de technische managers, een groep met communicatieverantwoordelijken en een groep voor het management. De helft van het werk bij de aanpak van een incident zal gaan over coördinatie en communicatie.

4. Stel een crisismanagementteam samen

Het crisisbeheerteam coördineert alle activiteiten die nodig zijn om uw IT-systemen weer operationeel te maken, maar houdt zich ook bezig met zakelijke, IT-prioriteiten, communicatie en juridische aspecten.

Stel een crisismanagementteam samen (soms ook bedrijfscontinuïteitsteam genoemd) dat afspraken maakt over bedrijfsprofessionals, communicatiestrategie, juridische kwesties en helpt bij het oplossen van prioriteitsconflicten bij het herstel van bedrijfsfuncties.

Dit team moet alle interne en externe communicatie coördineren en ervoor zorgen dat er tijdens de crisis met één stem wordt gesproken.

Het crisismanagementteam bestaat uit de belangrijkste zakelijke stakeholders, uw DPO, communicatie, juridische zaken en een IT-vertegenwoordiger. Benoem een crisismanager die als verbindingspersoon zal fungeren met uw technische team(s) en het crisismanagementteam.

Afhankelijk van de omvang van de organisatie kunt u overwegen twee crisismanagementteams te hebben, één voor de zakelijke aspecten en één voor de operationele IT-aspecten (waarbij het laatste team rechtstreeks aan het crisismanagement rapporteert).

5. Activeer het cyber incident response team

Roep de hulp in van cyberspecialisten, zoals forensische experts, die kunnen helpen vaststellen hoe het incident heeft plaatsgevonden en herhaling kunnen voorkomen.

Ga na of de reactie op incidenten deel uitmaakt van uw verzekeringscontract.

Ga na of u over interne deskundigheid beschikt, of huur anders een professioneel incident response team in om u te helpen bij de beoordeling van de aanvalsvector en het punt van binnendringing, en de juiste mitigatie mogelijk te maken.

6. Communiceer vroeg en vaak

Communiceer vroeg en vaak, houd uw interne medewerkers, leveranciers, dienstverleners en uw klanten op de hoogte. Het verbergen van deze aanval is over het algemeen geen goed idee, omdat het de reputatie van uw merk kan schaden.

Wees zo transparant mogelijk naar uw werknemers, belanghebbenden, klanten of gebruikers, en de pers over de aanval. Zelfs als u niet alle antwoorden hebt, is het belangrijk om al uw belanghebbenden te informeren. Meer informatie: https://www.cert.be/en/crisis-communication-event-cyber-attack

Als uw communicatiesystemen niet beschikbaar zijn, kunt u tijdelijke oplossingen overwegen, zoals het opzetten van een communicatie-webpagina of massameldingssystemen op basis van SMS.

7. Onderzoek de wettelijke verplichtingen

Ransomware actoren willen niet alleen dat u het losgeld betaalt om de systemen te ontsleutelen, maar hebben ook vaak gegevens geëxfiltreerd en zullen dreigen deze te verkopen of publiek beschikbaar te maken als u niet betaalt.

Er zijn wettelijke verplichtingen om autoriteiten zoals de DPA/GBA/APD in kennis te stellen van vermoedelijke inbreuken op de gegevensbescherming (doorgaans binnen 72 uur). https://www.gegevensbeschermingsautoriteit.be/burger/acties/contact (Website in NL en FR beschikbaar). Betrek uw functionaris voor gegevensbescherming (DPO) erbij.

Het juridische team en/of de functionaris voor gegevensbescherming kunnen ook een klacht indienen bij de plaatselijke politie.

8. Onderzoek de integriteit van de back-ups

Controleer of de aanvallers niet ook de beveiliging en de integriteit van uw back-upsysteem hebben aangetast.

Als het back-upsysteem veilig is, wat betekent dat u een onafhankelijke en geverifieerde kopie van uw gegevens hebt, is het vermijden van de betaling van ransomware de aanbevolen en beste optie. Daarom moet u de bevestiging hebben dat de back-ups niet zijn gecompromitteerd of benaderd (onveranderlijke back-ups zijn een must).

9. Coördineer de reactie op de hackers

In principe moet u GEEN losgeld betalen aan criminele organisaties.

Het Centrum voor Cybersecurity België (CCB) raadt de betaling van losgeld sterk af. Er kunnen zich situaties voordoen waarin betaling de enige optie is, maar houd er rekening mee dat de aanvallers zeer waarschijnlijk geïnteresseerd zijn in financieel gewin, dus alle mogelijkheden om u meer geld af te persen zullen ze proberen.

Wees voorzichtig in de omgang met de aanvaller. Het inhuren van een professionele onderhandelaar is geen wondermiddel. Er zijn veel gevallen bekend van losgeldbedragen die werden verdubbeld nadat een onderhandelaar was ingehuurd en onthoud altijd dat er geen garantie is dat u de ontcijferingssleutels ontvangt.

10. Over beperkende maatregelen

Implementeren van (minimale) beveiligingsmonitoringdiensten (SOC-dienst), activeren van een Endpoint Detection. Patch, reset, update bekende kwetsbare systemen die door de aanval zijn geraakt. Implementeer Multi-Factor Authenticatie.

Open geen internetconnectiviteit voor alle gebruikers, maar concentreer u eerst op de gebruikers die nodig zijn om uw IT-activiteiten of uw crisisbeheersingsfuncties te herstellen.

Patch, reset en update bekende kwetsbare systemen die door de aanval zijn getroffen. Voer een volledige reset van alle wachtwoorden uit en implementeer Multi-Factor Authentication, indien dit nog niet is gebeurd. Concentreer u eerst op geprivilegieerde accounts en diensten (beheeraccounts, beheerdiensten).

Implementeer security monitoring services (SOC service), activeer een Endpoint Detection oplossing van de kritische systemen zoals de Authenticatie, Autorisatie systemen, de systemen die Internet-Facing zijn. Het punt is dat u (beter) zicht wilt hebben op activiteiten die op uw netwerk plaatsvinden.

11. Begin met de wederopbouw van het systemen

Patch, update, herbouw en reset uw verificatiesysteem, implementeer Multi-Factor Authenticatie

Herstel een systeem niet op basis van back-ups van vlak voor of na de aanval. Handel eerst de vorige punten af en begin dan pas activiteiten om uw systeem vanaf back-ups opnieuw op te bouwen.

Zorg ervoor dat schone systemen tijdens het herstel niet opnieuw worden geïnfecteerd. Als het systeem eenmaal hersteld is, controleer dan of er niets schadelijks meer op staat voordat u het weer in uw netwerk opneemt. Herstel uw systemen op basis van een prioritering van kritieke diensten, herstel eerst servers dan endpoints. Het is ook aan te raden een kopie van uw versleutelde gegevens te bewaren, wellicht komt er in de toekomst een gratis decryptietool voor uw ransomware beschikbaar.

Verwijderen of volledig isoleren van verouderde systemen en protocollen.

12. Herziening en toevoeging van extra beveiligingen om een toekomstige aanval te voorkomen

Hoewel de nadruk ligt op het herstellen van de aanval en het opnieuw opbouwen van de infrastructuur, moet het management zich ervan bewust zijn dat een nieuwe aanval mogelijk is.

Neem de tijd om de aanval in detail te analyseren en te documenteren, en voer nieuwe controles, processen, procedures en oplossingen in om een volgende aanval te voorkomen.

Webinar beschikbaar in het Nederlands en Frans: https://www.youtube.com/watch?v=r0Iraugn-wo

CERT.be ransomware brochure beschikbaar in het Nederlands en Frans.

Contact

Centrum voor Cybersecurity België
Wetstraat 16
1000 Brussel
info@ccb.belgium.be

Disclaimer

Deze gids en de bijbehorende documenten zijn opgesteld door het Centrum voor Cybersecurity België (CCB), een federale overheidsdienst opgericht bij koninklijk besluit van 10 oktober 2014 en onder het gezag van de eerste minister.

De verstrekte informatie:

- is uitsluitend van algemene aard en heeft niet tot doel alle specifieke gevallen te behandelen;
- is niet noodzakelijk op alle punten volledig, nauwkeurig of up-to-date.

Verantwoordelijke uitgever

Centrum voor Cybersecurity België
M. De Bruycker, Directeur
Wetstraat, 16
1000 Brussel