willux.be
we keep IT zen

Incident Response Guide

De 10 stappen voor een effectief plan bij een cybersecurity incident

Wat is de beste manier om te voorkomen dat een cyberaanval uitdraait op een volledige inbraak? Bereid je van tevoren voor.

Na een hack realiseren organisaties zich vaak dat ze veel kosten en pijn hadden kunnen voorkomen als ze een effectief incident response plan hadden gehad.

Deze gids is bedoeld om je te helpen het kader voor cybersecurity incident response planning op te maken teneinde u de beste kans te geven om hackers te dwarsbomen. Deze aanbevelingen zijn gebaseerd op de praktijkervaringen van het Sophos Rapid Response-teams, zij hebben tienduizenden uren ervaring mbt de aanpak van cyberaanvallen.

Cybersecurity incident response plan

Er zijn 10 belangrijke stappen voor een effectief incidentbestrijdingsplan.

willux.be
we keep IT zen

Cybersecurity incident response plan

1. Bepaal de belangrijkste stakeholders
2. Identificeren van essentiële middelen
3. Table-top oefeningen uitvoeren
4. Beschermende middelen inzetten
5. Zorgen voor maximale zichtbaarheid
6. Toegangscontrole invoeren
7. Investeren in onderzoeksinstrumenten
8. Vaststellen van responsmaatregelen
9. Bewustmakingstraining geven
10. Managed security service activeren

1. Bepaal de belangrijkste stakeholders

Een goede planning voor een potentieel incident is niet enkel en alleen de verantwoordelijkheid van uw beveiligingsteam. In praktijk zal een incident hoogstwaarschijnlijk gevolgen hebben voor bijna elke afdeling van uw organisatie, vooral als het incident uitmondt in een grootschalige inbraak. Om een aanpak goed te coördineren, moet u eerst bepalen wie erbij betrokken moet worden. Dit omvat vaak vertegenwoordigers van het senior management, beveiliging, IT, juridische zaken en public relations.

Vooraf moet worden bepaald wie er bij de planning van uw organisatie moet worden betrokken. Bovendien moet een communicatiemethode worden gedefinieerd om een snelle respons te garanderen. Hierbij moet rekening gehouden worden dat uw normale communicatiekanalen (bijv. bedrijfsmail) door het incident kunnen worden beïnvloed en mogelijks onbruikbaar zijn.

2. Identificeren van essentiële middelen

Om de omvang en impact van een aanval te bepalen, moet uw organisatie eerst de bedrijfsmiddelen met de hoogste prioriteit in kaart brengen. Het in kaart brengen van uw belangrijkste middelen zal u niet alleen helpen bij het bepalen van uw beschermingsstrategie, maar maakt het ook veel eenvoudiger om de omvang en impact van een aanval te bepalen. Bovendien kan uw incident response team, doordat de meest kritieke bedrijfsmiddelen vooraf werden geïdentificeerd, zich tijdens een aanval focussen op deze, waardoor de verstoring van het bedrijf tot een minimum wordt beperkt.

3. Table-top oefeningen uitvoeren

Net zoals bij vele andere disciplines: oefening baart kunst. Hoewel het moeilijk is om de intense druk die uw team tijdens een potentiële inbraak ervaart volledig te simuleren, zorgen praktijkoefeningen voor een beter gecoördineerde alsook effectievere reactie wanneer zich een echte situatie voordoet. Het is belangrijk om niet alleen technische oefeningen te houden maar ook bredere oefeningen waarbij de verschillende zakelijke belanghebbenden worden betrokken die eerder zijn geïdentificeerd.

Bij table-top oefeningen moet de reactie van uw organisatie op verschillende scenario's worden getest. Elk van deze scenario's kan ook belanghebbenden omvatten buiten het directe technische team. Uw organisatie moet vooraf bepalen wie moet worden geïnformeerd wanneer een aanval wordt ontdekt, zelfs als deze met succes werd verdedigd.

Veel voorkomende incident response scenario's zijn:

- **Actieve aanvaller ontdekt**: In dit scenario is het essentieel dat het respons team vaststelt hoe een aanvaller uw omgeving heeft kunnen infiltreren, welke tools en technieken zij hebben gebruikt, wat het doelwit was, en of zij volharding hebben vastgesteld. Deze informatie helpt bij het bepalen van de juiste methodiek om de aanval te neutraliseren. Hoewel het voor de hand ligt om de aanvaller onmiddellijk uit de omgeving te verwijderen, kiezen sommige beveiligingsteams
- **Succesvolle inbraak:** Als een succesvolle data inbraak wordt ontdekt, moet uw team kunnen bepalen wat er gecompromitteerd is en hoe. Op basis hiervan kan de juiste reactie worden bepaald, inclusief de mogelijke gevolgen voor het beleid op het gebied van compliance en regelgeving, indien er contact moet worden opgenomen met klanten en of er juridische of rechtshandhavingsinstanties bij betrokken moeten worden.
- **Succesvolle ransomware-aanval:** Als kritieke gegevens en systemen zijn versleuteld, moet uw team een plan volgen om deze verliezen zo snel mogelijk te herstellen. Dit moet een proces omvatten om systemen te herstellen vanaf back-ups. Om te voorkomen dat de aanval wordt herhaald zodra u weer online bent, moet het team onderzoeken of de toegang van de aanvaller is afgesneden. Daarnaast moet uw organisatie bepalen of zij bereid is om in extreme situaties losgeld te betalen en, zo ja, hoeveel zij daarvoor over heeft.
- **Systeem met hoge prioriteit gecompromitteerd:** Wanneer een systeem met hoge prioriteit is gecompromitteerd, kan uw organisatie mogelijk niet langer normaal functioneren. Naast alle stappen die nodig zijn als onderdeel van een incident response plan, moet uw organisatie ook overwegen een business recovery plan op te stellen om minimale verstoring in dit scenario te garanderen.

4. Beschermende middelen inzetten

De beste manier om met een incident om te gaan is door u er in de eerste plaats tegen te beschermen. Zorg ervoor dat uw organisatie beschikt over de juiste endpoint-, netwerk-, server-, cloud-, mobiele en e-mailbescherming.

5. Zorgen voor maximale zichtbaarheid

Zonder het juiste inzicht in wat er tijdens een aanval gebeurt, zal uw organisatie moeite hebben om adequaat te reageren. Voordat een aanval plaatsvindt, moeten IT- en beveiligingsteams ervoor zorgen dat ze inzicht hebben in de omvang en impact van een aanval, met inbegrip van het bepalen van de aanvallers hun toegang en de systemen waarop ze toegang hebben. Een goede zichtbaarheid omvat het verzamelen van logboekgegevens, met de nadruk op endpoint- en netwerkgegevens. Aangezien veel aanvallen pas na dagen of weken worden ontdekt, is het belangrijk dat u historische gegevens heeft die dagen of weken (zelfs maanden) teruggaan om te onderzoeken. Zorg er bovendien voor dat van dergelijke gegevens een back-up wordt gemaakt, zodat ze toegankelijk zijn tijdens een actief incident.

6. Toegangscontrole invoeren

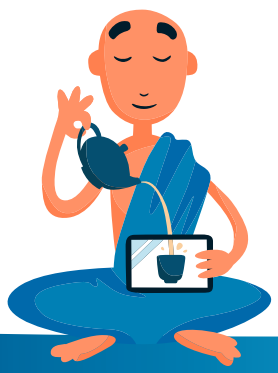
Aanvallers kunnen zwakke toegangscontrole gebruiken om de verdediging van uw organisatie te infiltreren en privileges te verhogen. Zorg dat u over de juiste middelen beschikt om de toegang op regelmatige basis te controleren. Dit omvat, maar is niet beperkt tot, het inzetten van multifactor authenticatie, beheerdersrechten beperken tot zo weinig mogelijk accounts (volgens het Least Privilege Principle), het wijzigen van standaardwachtwoorden en het verminderen van het aantal toegangspunten dat u moet bewaken.

7. Investeren in onderzoeksinstrumenten

Uw organisatie moet niet alleen zorgen voor de nodige zichtbaarheid, maar ook investeren in tools die tijdens een onderzoek de nodige context bieden.

Enkele van de meest gebruikte tools voor incident response zijn endpoint detection and response (EDR) of extended detection and response (XDR), waarmee u in uw omgeving kunt zoeken naar "indicators of compromise (IOC's)" en "indicators of attack (IOA)". EDR-tools helpen analisten vast te stellen welke bedrijfsmiddelen zijn aangetast, wat weer helpt bij het bepalen van de impact en omvang van een aanval. Hoe meer gegevens er worden verzameld - van de endpoints en daarbuiten - hoe meer context er beschikbaar is tijdens het onderzoek. Met een breder overzicht kan uw team niet alleen bepalen wat het doelwit van de aanvallers was, maar ook hoe ze toegang tot de omgeving hebben gekregen en of ze nog steeds toegang kunnen krijgen.

Naast EDR-tools kunnen geavanceerde beveiligingsteams ook een SOAR-oplossing (Security Orchestration, Automation and Response) inzetten die helpt bij responsworkflows.



8. Vaststellen van responsmaatregelen

Het detecteren van een aanval is slechts een deel van het proces. Om adequaat op een aanval te kunnen reageren, moeten uw IT- en beveiligingsteams ervoor zorgen dat zij een breed scala aan herstelacties kunnen uitvoeren teneinde de aanvaller te verstoren en te neutraliseren.

Responsacties omvatten, maar zijn niet beperkt tot:

- Getroffen hosts isoleren
- Blokkeren van schadelijke bestanden, processen en programma's
- Blokkeren van command and control (C2) en kwaadaardige website activiteiten
- Gecompromitteerde accounts bevriezen en aanvallers de toegang ontzeggen
- Opruimen van aanvallers artefacten en tools
- Sluiten van toegangspunten en gebieden waar aanvallers gebruik van maken (intern en van derden)
- Aanpassen van configuraties (bedreigingsbeleid, inschakelen van endpointbeveiliging en EDR op onbeschermde apparaten, aanpassen van uitsluitingen, enz.)
- Aangetaste bedrijfsmiddelen herstellen via offline back-ups

9. Bewustmakingstraining geven

Hoewel geen enkel trainingsprogramma ooit 100% effectief zal zijn tegen een vastberaden aanvaller, helpen educatieve programma's (zoals security & phishing awareness trainingen) uw risiconiveau te verlagen en het aantal waarschuwingen waarop uw team moet reageren te beperken. Het gebruik van tools om phishing-aanvallen te simuleren biedt uw personeel een veilige manier om een phish te ervaren (en er mogelijk het slachtoffer van te worden), zodat degenen die falen kunnen worden opgeleid en risicovolle gebruikersgroepen kunnen worden geïdentificeerd die aanvullende training nodig hebben.

10. Managed security service activeren

Veel organisaties zijn niet uitgerust om zelf incidenten af te handelen. Voor een snelle en effectieve respons zijn ervaren specialisten nodig. Om ervoor te zorgen dat u adequaat kunt reageren, kunt u overwegen een beroep te doen op een externe partner zoals Willux.be NV in combinatie met Sophos teneinde u een 24/7 bescherming te kunnen bieden.

willux.be
we keep IT zen

MDR-providers bieden 24/7 opsporing van bedreigingen, onderzoek en respons op incidenten als een beheerde dienst. MDR-diensten helpen uw organisatie niet alleen te reageren op incidenten voordat het een inbraak wordt, maar helpen ook de kans op een incident te verkleinen. MDR-diensten worden erg populair: volgens Gartner* zal in 2025 50% van de organisaties MDR-diensten gebruiken (dit is een stijging ten opzichte van minder dan 5% in 2019).

Data Forensic Incident Response (DFIR) diensten worden soms ook ingehuurd na een incident om bewijsmateriaal te verzamelen ter ondersteuning van een juridische of verzekeringsclaim.

Samenvatting

Wanneer een cyberbeveiligingsincident plaatsvindt, is tijd van essentieel belang. Een goed voorbereid en goed begrepen responsplan dat alle belangrijke partijen onmiddellijk in werking kunnen stellen, zal de impact van een aanval op uw organisatie drastisch verminderen.

Het MDR-team van bedreigingsjagers en responsdeskundigen:

- Speurt proactief naar en valideert potentiële bedreigingen en incidenten
- Gebruikt alle beschikbare informatie om de omvang en ernst van bedreigingen te bepalen
- Past de juiste bedrijfscontext toe voor geldige bedreigingen
- onderneemt acties om bedreigingen op afstand te verstoren, in te dammen en te neutraliseren
- Geeft bruikbaar advies om de hoofdoorzaken van terugkerende incidenten aan te pakken.

SOPHOS
Gold Partner

DIENSTVERLENER VOOR DE
KMO-PORTEFEUILLE

Willux.be is erkend dienstverlener voor de KMO-PORTEFEUILLE.
Registratienummer voor analyse: DV.A222546
Registratienummer voor opleiding: DV.O244638

Plan je ZEN moment

Willux.be NV
Hogendries 38
B-9450 Heldergem

+32 53 78 25 75
info@willux.be
https://willux.be

we love to connect