Incident Response voor preventie

Bedrijven in Nederland vertrouwen sterk op hun cyberweerbaarheid, maar is dat gegrond? Hoe worden zij weerbaarder dankzij Incident Responsemethoden?

kaspersky.nl
www.securelist.com

kaspersky BRING ON THE FUTURE

Methodiek

Dit onderzoek is in juli 2023 namens Kaspersky uitgevoerd door PanelWizard. In totaal zijn 311 besluitvormers in de Nederlandse IT bevraagd over Incident Response en cyberbeveiliging.

TOP 5 inzichten

1. **Er ontbreken standaard beveiligings-maatregelen**
   Een groot aantal Nederlandse bedrijven zijn niet voorbereid op de gangbare beveiligings-uitdagingen. Opmerkelijk genoeg geldt bij 35% van deze bedrijven geen wachtwoordbeleid of is er geen nalevingstoezicht, waardoor ze kwetsbaar zijn voor cyberaanvallen. Slechts 33% heeft een adequaat patchbeheerbeleid en hoewel 72% regelmatig back-ups maakt, voert slechts 26% aanvalssimulaties uit en een nog kleiner deel (17%) heeft een zero-trustbeleid

2. **Nederlandse bedrijven zijn onvoorbereid om risico's te beperken**
   Hoewel 45% van de geïnterviewde bedrijven overtuigd zijn dat ze een cyberaanval binnen 60 minuten kunnen ontdekken, maakt 41% van de bedrijven in dit onderzoek geen gebruik van anti-phishingsoftware, waardoor ze zichzelf blootstellen aan een groter risico op social engineering-aanvallen. Bovendien traint de helft van de bedrijven zijn medewerkers niet regelmatig over onderwerpen als spam of phishing, waardoor er risico's ontstaan

3. **Gebrek aan gereedheid van Incident Response**
   De standaard beveiligingsmaatregelen, zoals een robuust wachtwoordbeleid, protocollen voor databack-up en meerfactorauthenticatie ontbreken bij een groot aantal van de Nederlandse respondenten. Aanvullend heeft slechts 43% van de organisaties richtlijnen voor het documenteren van beveiligingsincidenten: een fundamentele stap in het vaststellen van effectieve Incident Responsestrategieën. Minder dan de helft heeft een plek gedefinieerd waar incidenten worden vastgelegd en slechts 38% gebruikt tools voor de initiële analyse van beveiligingsincidenten.

4. **Ontoereikende cyberverzekerings- en Incident Responseplannen**
   Hoewel minder dan 3% van de respondenten vindt dat het maken van een Incident Responseplan een verspilling van geld en tijd is, heeft slechts 29% Incident Responseplannen geformuleerd en geeft 30% aan dat stakeholders in hun organisatie geen duidelijk gedefinieerde rollen hebben in het geval van een cyberincident. Slechts 16% van de bedrijven heeft een cyberverzekering om potentiële schade te dekken, iets dat nog verder versterkt wordt door de uitdagingen tijdens beveiligings-inbraken en cyberaanvallen.

5. **Overmoed en gebrek aan bewustzijn**
   Er ontstaat een paradox bij IT-besluitvormers, hetgeen tekenend is voor de overmoed en het gebrek aan bewustzijn. Terwijl 67% gelooft dat Incident Responseplannen en tools aanvallen hebben afgehouden, gelooft 39% van de besluitvormers niet dat hun eigen beveili-gingsteam het risico van aanvallen op een juiste manier kan beoordelen. Nog zorgwekkender is dat slechts 22% denkt dat ze een inbraak in minder dan 30 minuten kunnen detecteren. Dit toont een mate van zelfvoldaanheid in het inschatten en inperken van risico's.

Voorwoord - Wake-up call voor Incident Response: Kritische tekortkomingen bij Nederlandse bedrijven onthuld

In deze hyperverbonden wereld is de beveiliging van je bedrijf geen optie meer. Terwijl de technologie evolueert, evolueren ook de tactieken van cybercriminelen, die continu slimmer worden en afhankelijker worden van nieuwe technologieën.

Ons meest recente onderzoek, waar meer dan 300 IT-besluitvormers in Nederland aan meededen, legt een sobere realiteit bloot: een aanzienlijk deel van de bedrijven in het land is slecht voorbereid om zich te beschermen tegen de nieuwste cyberbeveiligings-dreigingen. Dit rapport benadrukt enkele cruciale gebieden die direct moeten worden aangepakt: van de tekortkomingen in beveiligingsmaatregelen tot een gebagatelliseerd begrip van cyberrisico's.

Het moge duidelijk zijn dat de huidige staat van paraatheid voor Incident Response ongewenst is. Een verontrustend aantal bedrijven is niet adequaat voorbereid op het heersende beveili-gingslandschap of naleving van NIS2-standaarden. Te veel bedrijven hebben geen uitvoerig beleid voor veilige wachtwoorden of het afdwingen van nalevingsstandaarden. Deze nonchalante aanpak stelt organisaties bloot aan mogelijke infiltratie door cybercriminelen die kwetsbaarheden kunnen uitbuiten en ransom- en malware via de supply chain kunnen loslaten.

Als cybercriminelen een netwerkkwetsbaarheid benutten als startpunt voor een cyberaanval, krijgen organisaties te maken met twee uitdagingen. De eerste uitdaging is de snelle herkenning, analyse en beperking van de opgelopen schade. De tweede is de snelle oplossing om bedrijfscontinuïteit te garanderen. Het is aan het management van het bedrijf, in samenwerking met beveiligingsteams, om proactief een actieplan op te stellen in het geval van een cyberincident en de nasleep ervan. Hier begint de rol van Incident Response (IR).

IR omvat de georganiseerde pogingen om responsacties te initiëren als potentieel kwaadaardige activiteiten binnen het netwerk worden gedetecteerd. De fundering hiervoor wordt gelegd in een Incident Responseplan, waarin rollen worden gedefinieerd en een systematisch aanpak voor cyberbeveiligingsteams in kaart wordt gebracht om verschillende aanvalstypes te pareren, incidenten te detecteren en oplossingsstrategieën te implementeren.

Er zijn verschillende mogelijkheden voor het verfijnen van de detectiemethodieken en procedures voor een functionele cybersecurity Incident Response. Snelle actie bij aanvallen kan de potentiële gevolgen van een inbraak beperken en daarom zijn IR-strategieën, tools en services van onschatbare waarde.

IR overstijgt echter het pure incidentbeheer: het vormt een continu streven naar proactieve maatregelen die geleidelijk de algehele cyber-beveiliging vergroten. Dit rapport geeft een nauwgezette weergave van de huidige staat van cyberbeveiliging bij Nederlandse bedrijven, met een speciale nadruk op de voordelen van het proactief implementeren van IR-werkwijzen en tools.

Terwijl we dieper ingaan op de details van deze bevindingen, wordt de urgentie duidelijk van verbeterde beveiligingsmaatregelen en een genuanceerder begrip van evoluerende dreigingen. Daarom delen wij een uitgebreide uitleg over het ontwerp met besluitvormers en combineren we die met een pragmatische handleiding voor het maken van een Incident Responsedraaiboek: een fundamentele stap naar verhoogde cyberweerbaarheid.

Tim de Groot
Territory Manager
Benelux en Nordics bij
Kaspersky

Wat is Incident Response?

Als een bedrijf wordt aangevallen, moeten er twee uitdagingen worden opgelost. Aan de ene kant moet de schade worden beperkt en aan de andere kant moet de bedrijfscontinuïteit worden gewaarborgd. Daar komt Incident Response om de hoek kijken. Het reageert op een beveiligingsincident (Incident Response), maar het is meer dan dat. Het geeft een gedetailleerde weergave van het incident. Een Incident Responseservice zoals Kaspersky omvat het volledige incidentonderzoek en de responscyclus: van vroegtijdige Incident Response en bewijsverzameling naar het identificeren van aanvullende sporen van hackpogingen en het maken van een plan om de aanval tegen te gaan. In het algemeen bestaat een Incident Response uit zes fasen:

- **Voorbereiding:** Incident Response is geen proactieve reactie op een beveiligingsincident, maar een preventieve maatregel. Bedrijven bereiden zich vaak alleen voor op noodsituaties. Hieronder vallen ook Incident Responseplannen en draaiboeken, simulatieoefeningen of het afnemen van een cyberverzekering.

- **Detectie:** In deze fase wordt een incident geïdentificeerd en gerapporteerd en wordt informatie over het incident verzameld.

- **Beperking:** Afhankelijk van de beschikbare informatie wordt het incident ingedamd om te voorkomen dat het zich verder verspreidt in het zakelijke netwerk.

- **Eliminatie:** Schadebeperking wordt vergezeld door de uitschakeling van de aanval. Bestaande kwaadaardige bestanden worden van de geïnfecteerde apparaten verwijderd, de systemen worden versterkt met aanvullende beveiligings-maatregelen, updates worden toegepast en bestaande beveiligingsproblemen worden aangepakt.

- **Herstel:** In deze fase worden de systemen bijvoorbeeld hersteld nadat ze zijn ontkoppeld van de infrastructuur. Back-ups worden teruggezet.

- **Lessons Learned:** Na de aanval wordt weer vóór de aanval. Na een aanval worden alle stappen onderzocht en geanalyseerd: Wat ging er goed? Wat ging er niet goed? Op basis van die informatie worden de bestaande Incident Responseplannen, draaiboeken of controlelijsten bijgewerkt (zie punt één van de lijst, voorbereiding).

Bedrijven in Nederland zijn niet voorbereid op de huidige beveiligingsuitdagingen

Uit het meest recente onderzoek van Kaspersky onder 311 IT-besluitvormers in Nederland is gebleken dat een groot deel van de Nederlandse bedrijven niet voorbereid zijn op de huidige beveiligingsuitdagingen en ook niet voldoen aan de NIS2-vereisten. Hoewel 80% van de respondenten denkt dat preventieve maatregelen en goed gedefinieerde processen essentieel zijn voor een houdbare cyberbeveiliging en 58% denkt dat ze een hoge Incident Responseparaatheid hebben, laten de feiten een ander verhaal zien.

Meer dan een derde (35%) van de ondervraagde bedrijven hebben geen beleid voor veilige wachtwoorden en hebben geen controle op naleving. Onveilige wachtwoorden maken het makkelijker voor aanvallers om een netwerk binnen te dringen en ransomware of andere malware te introduceren. Het is ook zorgwekkend dat meer dan de helft van de bedrijven hun medewerkers niet regelmatig traint in onderwerpen als spam of phishing. Dit zijn de klassieke wegen van cybercriminelen om toegang tot gegevens te krijgen. De dagen van slecht geschreven spam-en phishingmails vol spelfouten zijn verleden tijd. Tegenwoordig zijn spam- of phishingmails nauwelijks te onderscheiden van echte berichten, voornamelijk vanwege tools zoals ChatGPT. Toch gebruikt 41% geen anti-phishingsoftware. Met de huidige beveiligingssituatie en een vrij constant hoog aantal phishingaanvallen stellen bedrijven zich bloot aan de risico's van ransomware-infecties.

Een aanvullend risico is dat 28% van de bedrijven geen back-ups van hun data maakt. Dit betekent dat in het geval een ransomwareaanval, of zelfs de vernietiging van een fysiek datamedium, dat de data niet meer beschikbaar is.

"Het is lastig te geloven dat er nog steeds bedrijven zijn die niet regelmatig back-ups van hun data maken", aldus Kai Schuricht, Lead Incident Response Specialist bij Kaspersky. "Voeg daaraan de combinatie van onveilige wachtwoorden en niet-getrainde medewerkers toe en ransomware kan een bedrijf snel naar de limieten van zijn economische weerbaarheid brengen. Het risico op een succesvolle aanval is in deze gevallen erg hoog."

Preventieve Incident Response? Ontbreekt in veel bedrijven

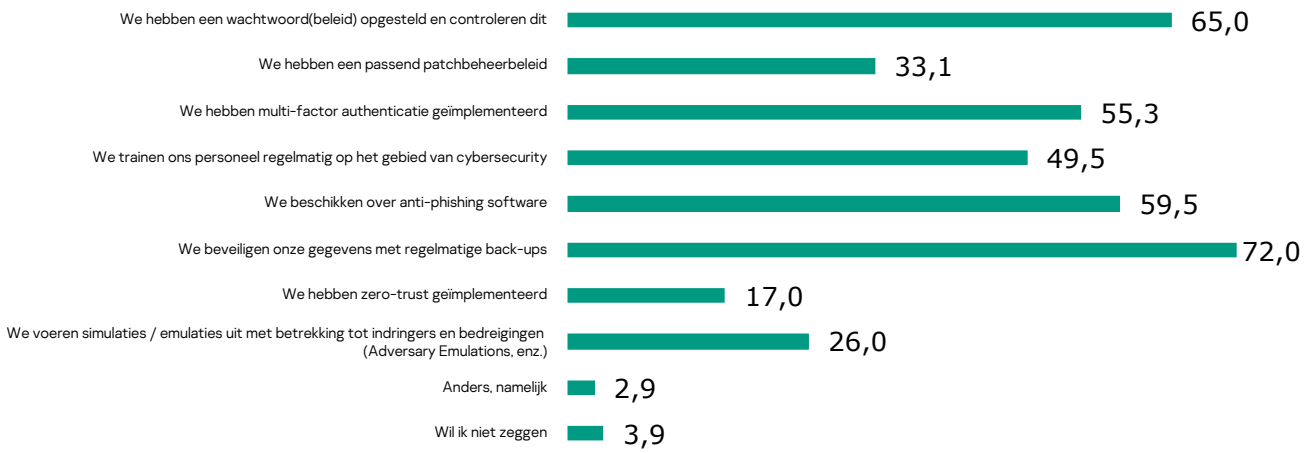
De status quo van beveiligingsmaatregelen bij sommige bedrijven in Nederland is ontnuchterend als je goed kijkt naar de resultaten in dit onderzoek. De meest fundamentele zaken, zoals wachtwoord-beleiden, het maken van back-ups of multifactor-authenticatie, zouden voor elke organisatie deel moeten uitmaken van de basisbescherming en moeten worden aangevuld met effectieve endpointbeveiliging. De realiteit is echter anders: respectievelijk 35%, 28% en 45% van de bedrijven beschikt hier niet over. Als het gaat om 'aanvullende maatregelen' tegen geavanceerde aanvallen, is het beeld nog slechter.

Uit het huidige onderzoek van Kaspersky blijkt dat nog niet eens de helft (43%) van alle ondervraagde bedrijven in Nederland richtlijnen hanteert over het documenteren van beveiligingsincidenten. Dit zou de eerste basis vormen voor het Incident Responsedraaiboek. Minder dan de helft van de organisaties (48%) heeft een incidentmeldpunt gedefinieerd. Slechts een derde van de respondenten (32%) gebruikt netwerksegmentatie om apparaten van elkaar te isoleren en slechts 38% gebruikt tools voor de initiële analyse van beveiligingsincidenten. Nog minder (32%) voert preventieve audits uit.

Nog zorgwekkender is dat de duizelingwekkende meerderheid (74%) van de bedrijven geen simulatie/emulatie uitvoert met betrekking tot dreigingen (via Table Top Exercise (TTX) of Adversary Emulations). Zonder kritische processen te testen, kunnen bedrijven er niet van uitgaan dat ze hulp of begeleiding kunnen bieden in het geval van noodsituaties. Het is niet verstandig om blindelings te vertrouwen op de functionaliteit van individuele componenten van de beveiligingsinfrastructuur, zonder deze services en processen regelmatig te testen via simulaties. Noodplannen en meldpunten zijn immers pas betrouwbaar als ook zeker is dat ze in geval van een calamiteit soepel en volgens plan functioneren.

Het is zorgwekkend dat slechts 29% van de bedrijven over Incident Responseplannen beschikt. Een vijfde (21%) van de ondervraagde bedrijven heeft een Incident Responsedraaiboek en 25% heeft een centraal gedocumenteerde opslagplaats voor

In ons bedrijf hebben wij de volgende maatregelen getroffen om cyberveiligheidsincidenten te voorkomen: (meervoudige selectie)



gecompromitteerde apparaten. Dit is belangrijk voor het onderzoek, omdat dit de enige manier is om de oorsprong van een aanval te identificeren. Omgekeerd betekent dit ook dat driekwart van de bedrijven niet gebruikmaakt van een repository. Dit maakt het traceren van de aanval en het herstellen van de schade veel moeilijker.

In een Incident Responsedraaiboek worden de acties gedefinieerd die bedrijven moeten ondernemen in het geval van een specifiek incident. Een Incident Responseplan is daarentegen toepasbaar op een breed scala aan incidenten. Deze plannen zijn ontworpen om een medewerker van een organisatie te helpen.

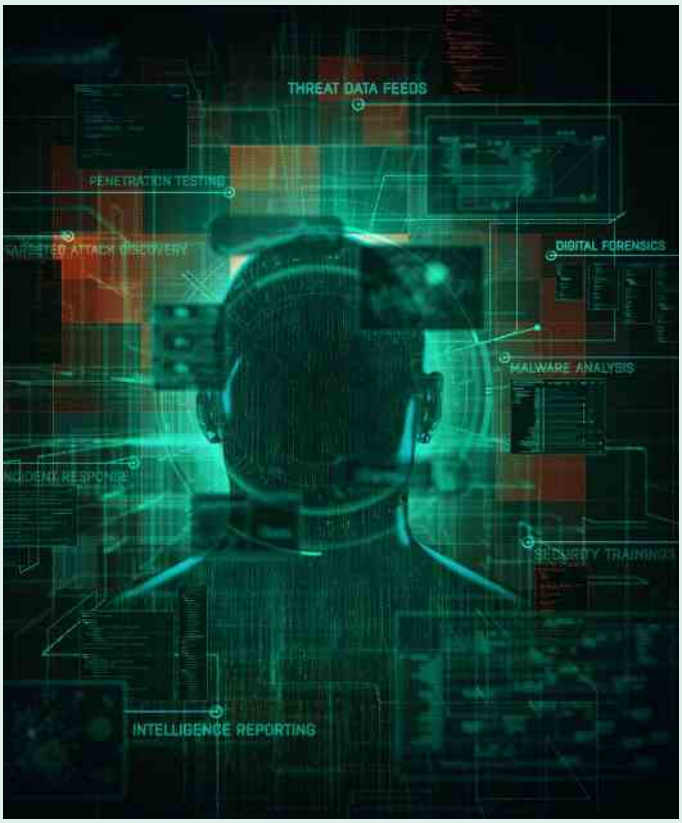
Momenteel heeft slechts een op de drie bedrijven (33%) een patchbeheerbeleid. Toch behoren beveiligingsproblemen in applicaties en besturingssystemen tot de meest voorkomende aanvalsvectoren in bedrijven. Met phishingaanvallen kunnen cybercriminelen data van netwerken stelen, bedrijven chanteren, lokaal beheerde servers en computers in gevaar brengen en deze in botnets integreren en vele andere schadelijke acties uitvoeren. Het Analistenrapport voor Incident Response van Kaspersky laat zien dat tijdig patchbeheer essentieel is.

'Patchen is altijd een uitdaging. Aan de ene kant is het relatief eenvoudig om beveiligingslekken te dichten, maar aan de andere kant is het proces meestal iets ingewikkelder dan je denkt", aldus Kai Schuricht, Lead Incident Response Specialist bij Kaspersky, over het gebrek aan patchbeheer bij bedrijven. "Als bedrijven besluiten hun systemen te updaten, kost dat tijd. Dat komt omdat de updates eerst getest, vrijgegeven en vervolgens gedistribueerd moeten worden. Dit kost tijd en vergroot uiteraard het tijdsbestek waarin de systemen kwetsbaar zijn. Het tijdvenster voor succesvolle aanvallen wordt ook verlengd. Een goed doordacht en dus efficiënt patchbeheer kan hierbij ondersteunen en tegelijkertijd rekening houden met de verschillende eisen van bijvoorbeeld IT-beveiliging en productie."

Bovendien hanteert slechts 17% van alle bedrijven een zero-trustaanpak, waarbij gebruikers en beheerders alleen de rechten krijgen die ze daadwerkelijk nodig hebben in hun rol en werk. Tegelijkertijd wordt ervoor gezorgd dat authenticatie- en beveiligingscontroles zo vaak mogelijk plaatsvinden. Als aanvallers inloggegevens in handen krijgen in een omgeving zonder zero-trust, kunnen ze zich veel eenvoudiger door het netwerk verplaatsen en systemen, zonder tussenkomt, in gevaar brengen. Volgens het onderzoek lijkt dit momenteel mogelijk bij ruim 83% van de bedrijven in Nederland.

Vertrouwen en overmoed: zijn IT-besluitvormers het probleem?

Uit het onderzoek van Kaspersky blijkt dat IT-besluitvormers veel vertrouwen hebben in hun eigen beveiligingsteam als het gaat om het beoordelen van risico's en bedreigingen in het cyberuniversum. Volgens het onderzoek is 82% van de besluitvormers van mening dat hun eigen beveiligingsteam in staat is om de risico's van aanvallen correct in te schatten. Hiervan vindt 18% zelfs dat hun team uitstekend is, en vertrouwt erop dat ze de risico's zelf inschatten.



Hetzelfde geldt voor vaardigheden als het identificeren en prioriteren van kwetsbaarheden en risico's (85%), het isoleren van getroffen systemen (85%) en het uitvoeren van back-ups (88%). Hoewel besluitvormers vinden dat hun beveiligingsteam hierop voldoende scoort, is een klein deel er zelfs van overtuigd dat hun team het daadwerkelijk uitstekend doet (respectievelijk 21%, 20% en 28%), wat laat zien dat er veel vertrouwen is.

Een ander signaal van vertrouwen is de snelheid waarmee een cyberincident wordt geëlimineerd. De meerderheid van de respondenten (65%) denkt dat ze een aanval binnen 24 uur kunnen beheersen en de gevolgen kunnen elimineren, terwijl 25% zelfs denkt dat ze dit binnen een uur kunnen doen. Kai Schuricht deelt deze mening niet. Zijn reactie op basis van jarenlange ervaring: "Dat is een stevige aanname!" Het onderzoeken van een aanval die langer dan een week heeft geduurd, duurt namelijk gemiddeld al ruim 60 uur.

Jornt van der Wiel, Senior Security Researcher, Global Research and Analysis Team bij Kaspersky deelt zijn mening: "Het is ongelooflijk naïef dat iets minder dan 50% van de respondenten denkt een aanval binnen een uur te kunnen detecteren. Zeker gezien de defensieve maatregelen die de meeste respondenten hebben genomen. Door staten gesponsorde groepen en complexe criminele organisaties zijn zo succesvol, omdat ze niet worden opgespoord. Vooral door staten gesponsorde groepen kunnen zich op netwerken begeven voordat ze uiteindelijk ontdekt worden, wat vaak gebaseerd is op geluk en niet op preventieve maatregelen en strenge beveiliging."

Tussen voorbereiding en nalatigheid - Incident Responsecapaciteit: Slecht

Als het gaat om kennis, voorbereiding en implementatie van IR-services blijkt er sprake te zijn van een grote tegenstrijdigheid. Terwijl meer dan driekwart (77%) van de besluitvormers zegt te weten wat IR-services en -tools zijn, en ook de meerderheid (67%) ervan overtuigd is dat hun IR-services en -tools een of meer incidenten hebben voorkomen, blijkt er in de werkelijkheid een gebrek aan basismaatregelen om te zorgen voor voldoende cyberbeveiligingsparaatheid. Zo zegt 44% dat hun

organisatie geen cyberincidenten simuleert en/of hun IR-plannen niet test, terwijl 42% zegt dat hun organisatie niet over een hoge IR-gereedheid beschikt. Een kleiner aantal respondenten zegt dat ze daadwerkelijk een IR-plan hebben (29%) of dat er een draaiboek aanwezig is (21%).

Hoewel besluitvormers wel weten wat IR-services en -tools voor hun organisatie kunnen betekenen, blijft de implementatie achter en lijkt deze niet hoog op hun takenlijst te staan. Hoewel minder dan 3% van de respondenten van mening is dat het opstellen van een IR-plan tijd- en geldverspilling is, vindt iets minder dan 28% dat het hebben van een IR-plan onmisbaar is binnen hun organisatie. Een kleiner deel (20%) zegt hetzelfde over een IR-draaiboek. Uit de cijfers blijkt dat een hoog kennisniveau over IR niet automatisch betekent dat organisaties ook daadwerkelijk voorbereid zijn.

Voorkomen is beter dan nazorg. Dit betekent dat bedrijven moeten investeren in preventieve maatregelen voordat er zich een incident voordoet, en niet alleen als er sprake is van een acute aanval," aldus Kai Schuricht, Lead Incident Response Specialist bij Kaspersky. "Tegelijkertijd is het maken van IR-plannen niet zo ingewikkeld. Er zijn zelfs gratis sjablonen op het internet, bijvoorbeeld op www.IncidentResponse.org/playbooks/.

Foutencultuur: Begrip en training of straffen en consequenties?

Hoewel tweederde (65%) van de respondenten zegt dat er binnen hun bedrijf een goede foutencultuur bestaat en de algemene consensus stelt dat werknemers niet bang hoeven te zijn voor eventuele gevolgen, is slechts 19% van alle deelnemers aan de enquête het daar volledig mee eens. In sommige bedrijven kunnen werknemers die een phishingmail openen of op een malwarelink klikken, zelfs te maken krijgen met disciplinaire maatregelen. De uitspraken 'wordt afhankelijk van de situatie ontslagen', 'krijgt een waarschuwing' of 'krijgt een training' komen veelvuldig voor in de antwoorden van de respondenten.

"Een goede foutencultuur in het bedrijf is essentieel, zodat medewerkers beveiligingsincidenten direct melden. Een snelle reactie is immers cruciaal bij een IT-beveiligingsincident," aldus Kai Schuricht, Lead Incident Response Specialist bij Kaspersky. "Als er consequenties zijn voor werknemers, is de kans groot dat ze incidenten onderschatten of verbergen. Wel is het van belang dat verantwoordelijke partijen op tijd worden geïnformeerd over wangedrag of fouten, zodat de schade tot een minimum kan worden beperkt door efficiënt op de aanval te reageren."

Voorbeeldstructuur van een Incident Responseplan:

- Overzicht van Incident Responseplan
  - Incidentclassificatie:
  - Heldere definitie
  - 'Wat is een informatiebeveiligingsincident?'
  - Prioritering van incidenten (de prioriteit van een incident wordt gedefinieerd op basis van de potentiële impact op de volgende faciliteiten)
  - Bedrijfsprocessen
  - Gevoelige data
  - Opmars van de aanvaller (controle verkregen)
  - Heldere definitie van 'Incidentprioriteitsniveaus'
  - Kritisch 1, 2, 3, 4 (min of meer afhankelijk van de klant)
  - Toekenning van de gevolgen van een incident aan de prioriteitsniveaus van een incident
- Incidentcategorieën:
  - Phishing
  - Malware-uitbraak
  - Enz.
- Niveau van Incident Responseteam
- RACI-matrix van Incident Response
- In kaart brengen van Incident Response en Cyber Crisis Management Plan (CCMP)
- Incidentstatistieken en SLA's voor Incident Response:
  - Gedefinieerde tijden voor verschillende taken in het IR-plan.

Zo maak je een Incident Responsedraaiboek

Een draaiboek is ontworpen om het beveiligingsteam van een bedrijf in staat te stellen effectief en snel te reageren op cyberaanvallen. Afhankelijk van de organisatie bestaat het Incident Responseproces uit verschillende fases. Volgens NIST zijn dit: voorbereiding, detectie en analyse, insluiting, remediëring en herstel, en post-incidentactiviteiten.

Deze cycli kunnen worden onderverdeeld in 'actieblokken'. Deze blokken kunnen op hun beurt worden gecombineerd, afhankelijk van de specifieke aanval, om tijdig en efficiënt te reageren. Elke 'actie' is een eenvoudige instructie die een analist of een geautomatiseerd script volgt bij een aanval.

Stap 1: Incident Response voorbereiden

De eerste stap van elk draaiboek voor Incident Response gaat over de voorbereidingsfase van de NIST Incident Response Life Cycle. Het draait om Incident Response. Meestal gaat het om een aantal verschillende stappen, zoals incidentpreventie (kwetsbaarheidsbeheer, gebruikersbewustzijn of malwarepreventie). De waarschuwingsveldset en de visuele weergave ervan worden gedefinieerd. Voor elk type incident moeten verschillende veldsets worden opgesteld die het meest praktisch zijn voor het Incident Responseteam. Hiertoe worden voor een bepaald type incident specifieke rollen gedefinieerd, maar ook escalatiescenario's en de toewijzing van tools om contact op te nemen met stakeholders (bijvoorbeeld via e-mail, telefoon, WhatsApp of sms). Daarnaast heeft het Incident Responseteam voldoende toegang nodig tot beveiligings- en IT-systemen, analysesoftware en middelen.

Het is verstandig om automatiseringen en integraties te ontwikkelen en te implementeren die kunnen worden gestart vanuit een Security Orchestration, Automation and Response (SOAR)-systeem. Zo garandeer je een tijdige reactie en voorkom je menselijke fouten. In de detectiefase worden gegevens verzameld uit IT-systemen en -beveiligingstools, maar wordt ook publiek beschikbare informatie verzameld en informatie van mensen binnen en buiten de organisatie. Ook worden voorlopers en indicatoren geïdentificeerd.

Stap 2: Alomvattend onderzoeksproces opzetten

Daarna volgt analyse, waarbij documentatie, triage, onderzoek en melding betrokken zijn. De documentatie helpt het team bij het definiëren van de analysegebieden en hoe deze moeten worden ontworpen na ontdekking en registratie in het incidentbeheersysteem. Pas dan gaat het Incident Responseteam over tot triage om het incident te prioriteren, te categoriseren, te controleren op false-positives en te zoeken naar gerelateerde incidenten. Het grootste deel van de analysefase is het onderzoek, dat bestaat uit het verzamelen van logboeken, assets en verrijkende artefacten, en het definiëren van een incidentgebied.

Hier moeten alle gegevens over het incident beschikbaar zijn om patient zero en het toegangspunt te identificeren. Het team moet weten hoe een aanvaller ongeautoriseerde toegang heeft verkregen en welke host of welk account als eerste is gecompromitteerd. Dit helpt bij het inperken van de cyberaanval en het voorkomen van soortgelijke aanvallen in de toekomst. Door incidentdata te verzamelen, krijgen de verantwoordelijke partijen relevante informatie (zoals assets en artefacten als de hostnaam, het IP-adres, de bestandshash of de URL) die verband houden met het incident.

Daarmee kan het incidentgebied uitgebreid worden. Als het bereik van het incident wordt uitgebreid, kan het team de assets en artefacten verrijken met gegevens uit bronnen voor bedreigingsinformatie of lokale systemen met inventarisinformatie, zoals Active Directory, IDM of CMDB. Met behulp van een uitgebreid overzicht van de betrokken middelen kan het Incident Responseteam een risicobeoordeling maken en op basis daarvan de juiste vervolgacties ontwikkelen.

De beslissende factor is hoeveel hosts, gebruikers, systemen, bedrijfsprocessen of klanten zijn getroffen, en er zijn verschillende manieren om dit te escaleren. Als het risico middelgroot is, hoeven alleen de SOC-manager en enkele beheerders op de hoogte te worden gesteld om het incident te beperken. Als het risico op een incident kritisch is, moet het Incident Responseteam het crisisteam, hr of de toezichthouder op de hoogte stellen. Met deze melding is de analysefase voltooid. Alle stakeholders

moeten zo snel mogelijk op de hoogte worden gebracht van het incident, zodat de betreffende systeemeigenaar effectieve inperkings- en herstelmaatregelen kan nemen.

Stap 3: Inperken, verwijderen, herstellen

De derde fase omvat inperkings-, verwijderings- en herstelmaatregelen. Het hoofddoel van inperking is het onder controle houden van de situatie na een incident. Afhankelijk van de ernst van een incident en de mogelijke veroorzaakte schade moet het responsteam eerst passende inperkingsmaatregelen nemen. Na de voorbereidende fase waarin workflows werden gedefinieerd, is er nu een lijst met verschillende soorten objecten en mogelijke acties die kunnen worden ondernomen met de besproken tools. Nu moeten passende acties worden bepaald voor de gedocumenteerde acties op basis van de impact.

De totale schade hangt grotendeels af van deze fase, want hoe soepeler en preciezer de acties die in het draaiboek zijn gedefinieerd, hoe sneller gevaarlijke activiteiten kunnen worden geblokkeerd en de gevolgen ervan kunnen worden geminimaliseerd. Tijdens het insluitingsproces

worden verschillende acties ondernomen, zoals het verwijderen van een kwaadaardig bestand of het voorkomen van de activering ervan, het isoleren van een netwerkhost, het uitschakelen van een account of het scannen van een schijf met een antivirusprogramma. De keuze van de inperkingsmaatregelen is afhankelijk van het potentiële risico.

Daarom moet het Incident Responseteam voorzichtig zijn en bijvoorbeeld niet de wachtwoorden van alle accounts in het bedrijf opnieuw instellen als ze worden geconfronteerd met een brute-forceaanval. Soms beschikt het team niet over voldoende mogelijkheden om inbreuken te voorkomen, omdat ze geen machtigingen hebben voor bepaalde systemen. In dit geval is het verstandig om op acties te markeren waarvoor externe professionals, zoals systeembeheerders, L3-analisten of ondersteuningsteams, iteraties moeten uitvoeren en automatiseren.

De fases voor remediëring en herstel bestaan uit procedures om alles weer in gebruikt te nemen en ze zijn in veel opzichten vergelijkbaar. Het opschonen van eventuele tekenen van een aanval, zoals kwaadaardige bestanden of gemaakte geplande taken en services, is onderdeel van het remediëringsproces. De herstelfase is optioneel, omdat niet elk incident impact heeft op de infrastructuur. In deze fase moeten er wel gezondheidscontroles worden uitgevoerd en moeten de tijdens de aanval aangebrachte wijzigingen ongedaan worden gemaakt.

Stap 4: Leren van het incident

De laatste fase van het draaiboek gaat over de tijd na een incident en het daaruit voortvloeiende leereffect. Het doel ervan is om de ervaringen en geleerde lessen te gebruiken om het hele proces te optimaliseren. Deze taak kan worden vereenvoudigd door een reeks vragen te definiëren die het responsteam moet beantwoorden:

- Hoe goed heeft het Incident Responseteam het incident afgehandeld? - Welke informatie was eerder nodig?
- Had het team informatie beter kunnen delen met andere organisaties of afdelingen?

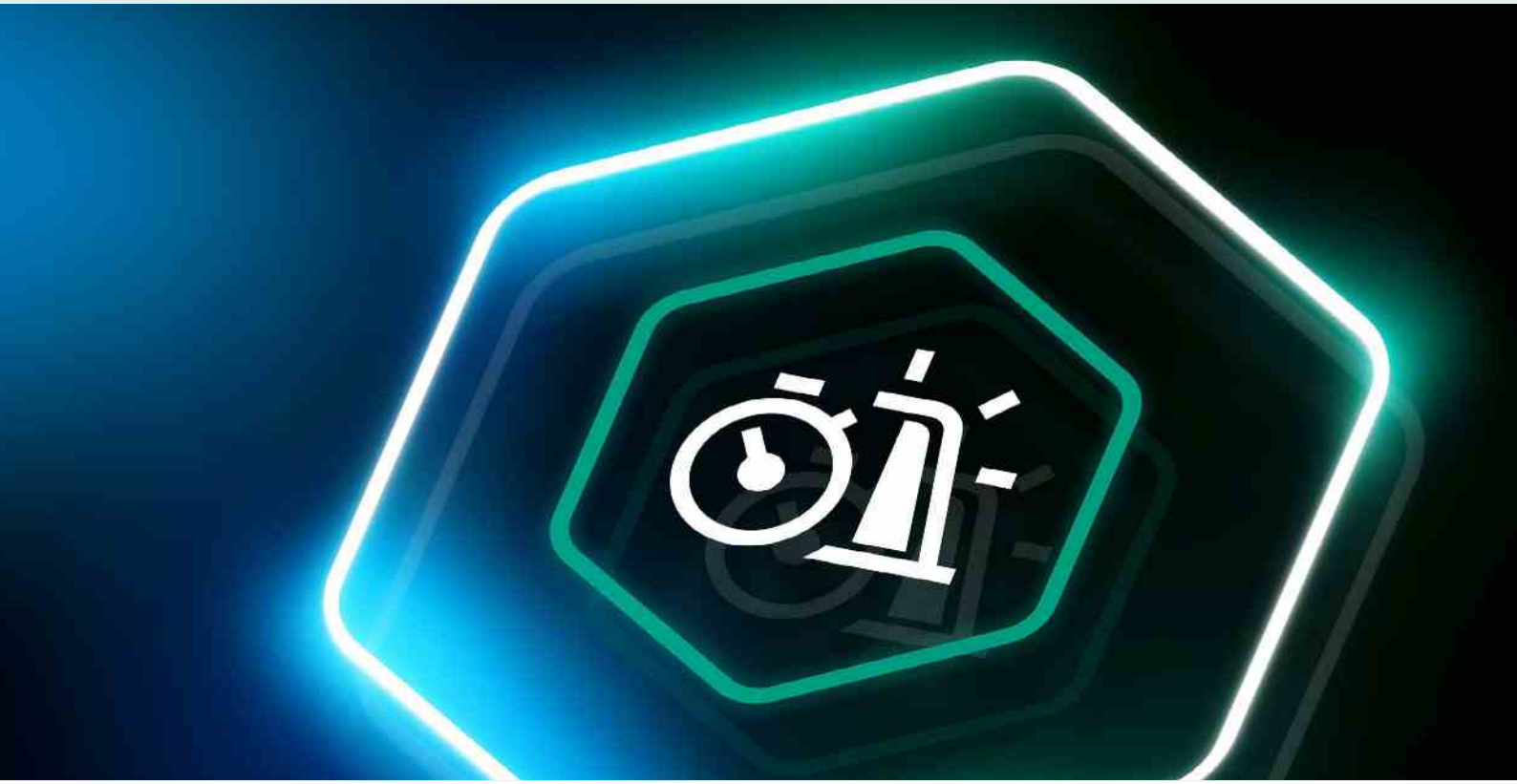
- Wat zou het team de volgende keer anders kunnen doen als hetzelfde incident zich voordoet?
- Welke aanvullende tools of middelen zijn nodig om soortgelijke incidenten in de toekomst te voorkomen of te beperken?
- Zijn er onjuiste handelingen verricht die schade hebben veroorzaakt of herstel hebben belemmerd?

Zodra al deze vragen zijn beantwoord, kan het responsteam de kennisbank bijwerken, detectie- en preventiemechanismen verbeteren of zelfs een nieuw responsplan ontwikkelen. Er ontstaat een cyclus van respons en preventieve actie die een bedrijf steeds cyberweerbaarder maakt.

Conclusie: Wat heb je nodig voor een goed IR-draaiboek?

Om een handleiding voor de respons op cyberveiligheidsincidenten te ontwikkelen, moeten het incidentbeheerproces en de bijbehorende fasen worden gedefinieerd. Hiervoor moeten tools/systemen worden gedefinieerd die helpen bij detectie, onderzoek, mitigatie, remediëring en herstel. Op basis van de gekozen tools worden acties gemaakt om logbestanden te verzamelen, inventarisinformatie of telemetrie van de getroffen assets te verrijken, hosts te isoleren, het opstarten van kwaadaardige bestanden te voorkomen, URL's te blokkeren, actieve sessies te beëindigen of accounts uit te schakelen. Verdere acties moeten gericht zijn op het wegnemen van tekenen van inbraak door het op afstand verwijderen van bestanden, en het verwijderen van verdachte services of geplande taken.

Daarna is het een kwestie van het herstellen van de systeemwerking door veranderingen ongedaan te maken en opgedane kennis over te dragen. Het is belangrijk om de verantwoordelijkheden binnen het Incident Responseteam te definiëren en ervoor te zorgen dat iedereen zijn specifieke rol kent. Op basis hiervan ontstaan procedures die het draaiboek vormen en doorgaans als volgt zijn gestructureerd: '<onderwerp> voert <actie> uit op <object> met behulp van <a tool>'. Alle onderwerpen, acties, objecten en tools zijn al gedefinieerd en zijn eenvoudig met elkaar te combineren. Ze vormen de individuele processen en die vormen op hun beurt de individuele elementen van een draaiboek.



kaspersky.nl
www.securelist.com

kaspersky BRING ON THE FUTURE