Anticiperen op de inbreuk

Wat te doen voor, tijdens en na een aanval.

INHOUD

- Voor 2
- Tijdens 3
- Na 4
- Conclusie 5

Aangeboden door, met complimenten van

Beveiligingsincidenten mogen dan onvermijdelijk zijn, de gevolgen van een gegevensinbreuk hoeven dat niet te zijn. De ernstigste inbreuken van vandaag de dag zijn vaak het resultaat van niet tijdige detectie, gebrekkige paraatheid met betrekking tot de beveiliging en een te late respons.

Wanneer organisaties hun mensen, processen en technologie niet integreren, kunnen ze niet zo snel een incident detecteren, erop reageren en voorkomen dat het zich tot een inbreuk ontwikkelt. Het resultaat? Een groter risico bij elk beveiligingsincident waar ze mee worden geconfronteerd.

Organisaties dienen over te gaan op een proactieve cyclus van voorbereiding, detectie en respons. Dit betekent dat organisaties moeten stoppen met het domweg meer technologie inzetten voor het bestrijden van het probleem. Ze moeten meer doen dan ad hoc reageren op incidenten op het moment dat deze zich voordoen. Ze dienen een holistische benadering te omarmen, een benadering die antwoord biedt op de fases voor, tijdens en na een potentiële inbreuk.

TechTarget Custom Media
EEN TECHTARGET WHITE PAPER

Voor

Bereid u vroeg en vaak voor: een degelijk responsprogramma bij incidenten is essentieel voor een organisatie die klaar wil zijn voor een inbreukscenario voordat een beveiligingsincident optreedt. Veel organisaties denken dat ze een draaiboek voor een inbreuk klaar hebben liggen, maar dit is meestal een handboek dat nooit is uitgetest. Voorbereiding betekent meer dan een document met vakjes om af te vinken dat lang geleden is opgesteld en nu ergens ligt te verstoffen. Het is een actief programma dat tijdens de voorbereidings- en responscyclus wordt gevoed door een aantal factoren.

Een organisatie dient manieren te vinden waarop ze hun programma kunnen bouwen, testen en verfijnen zodat een ieder die tijdens en na een inbreuk de geplande procedures moet uitvoeren, de procedures zo goed in de vingers heeft dat hij of zij ze in het geval van een echt incident als het ware slapend zou kunnen uitvoeren. Dit garandeert dat alle daarvoor aangewezen multifunctionele teams weten wat ze moeten doen op het moment dat de alarmbellen afgaan, zodat ze snel en effectief kunnen reageren.

Organisaties zouden dit beleid niet in een vacuüm moeten ontwikkelen. Als er in de toekomst incidenten plaatsvinden, dienen organisaties de geleerde lessen op te nemen in hun responsprogramma.

Bouw een effectief team: het kan een uitdaging zijn beveiligingsprofessionals te vinden met de noodzakelijke vaardigheden en ervaring, maar het is cruciaal een team op te zetten dat handelend op kan treden als er dingen fout gaan. Organisaties zouden het een prioriteit moeten maken hun mensen continu te laten groeien door hun vaardigheden te beoordelen, lacunes te identificeren en hen op een innovatieve manier te trainen. Hoe beter de leidinggevenden er in slagen het voorbereidingsproces boeiend te laten zijn, en er zelfs een teambuildings-ervaring van weten te maken, hoe meer dit proces bijdraagt aan het slimmer werken van de responsteams.

Als onderdeel van deze ontwikkeling is het zaak de beveiligingsteams een veilige leeromgeving te bieden waarin operationele ervaring op kunnen doen en ze beter leren begrijpen hoe aanvallers tegenwoordig denken. Dit draagt ertoe bij dat ze de motieven, hulpmiddelen en tactieken van de aanvaller beter begrijpen en verschaft ze kennis waarmee ze sneller incidenten kunnen voorkomen, detecteren, en er op reageren.

Integreer wereldwijde informatie: nu de vijanden van vandaag de dag steeds geavanceerdere hulpmiddelen, tactieken en procedures gebruiken om in een organisatie te infiltreren, moeten beveiligingsteams continu up-to-date en bewust zijn van vijandelijke trends en campagnes wereldwijd. Organisaties zouden een gedefinieerd informatieprogramma moeten ontwikkelen dat leidinggevenden op het gebied van de beveiliging, controleteams en de teams die op incidenten moeten reageren, op de hoogte houdt van huidige en opkomende bedreigingen, op zodanig wijze dat ze genoeg tijd hebben op effectieve wijze het risico te beoordelen en tegenmaatregelen te implementeren. Deze praktische informatie helpt organisaties uiteindelijk pro-actief te reageren in plaats van achter de feiten aan te lopen.

Implementeer realtime controle: hackers nemen geen pauze en ze werken niet binnen één specifieke tijdzone. Daarom is het noodzakelijk constant op de hoede te zijn om incidenten snel te detecteren en er snel op te reageren. Organisaties dienen 24 uur per dag, 7 dagen per week en 365 dagen per jaar hun systeem te controleren op bedreigingen. Leidinggevenden zouden zichzelf de vraag moeten stellen:

- Hebben ze de juiste infrastructuur en hebben ze de juiste mensen om geavanceerde bedreigingen rond de klok te detecteren?

- Is hun controleteam gewapend met de technische kennis en informatie over mogelijke aanvallen die hen helpt aanvallen sneller te detecteren en er sneller op te reageren?
- Is er een rechtstreekse lijn van de teams die op incidenten moeten reageren naar het controleteam zodat, wanneer een incident plaatsvindt, de kennis wordt gedeeld en er snel kan worden opgetreden? Zijn ze gewapend met relevante informatie over de bedreiging, informatie die hen helpt de dreiging te isoleren en uit te roeien?

Overweeg cyberverzekering: organisaties realiseren zich dat het risico op gegevensinbreuk nooit 100% kan worden uitgesloten. Wanneer er een inbreuk plaatsvindt, zijn organisaties verplicht zich te houden aan verschillende wetten met betrekking tot het melden van inbreuken, vooral in de Verenigde Staten en de Europese Unie. Om zich in te dekken tegen de financiële risico's die gepaard gaan met een inbreuk vullen bedrijven hun beveiligingsprogramma's aan met een cyberverzekering. Bedrijven doen er goed aan met hun verzekeringsagenten te bespreken welke maatregelen op het gebied van beveiligingsparaatheid, bedreigingsdetectie en respons bij incidenten hen een lagere verzekeringspremie kunnen opleveren.

Tijdens

Hoe sneller een incident wordt gedetecteerd en als kritisch wordt geprioriteerd, des te sneller kunnen resources worden toegewezen en kan er begonnen worden met responsactiviteiten. De detectiesnelheid tijdens een beveiligingsgebeurtenis kunnen het verschil maken tussen een klein incident en een grove inbreuk.

De vijanden van vandaag de dag voeren niet alleen brede aanvallen uit, waarbij ze kwetsbare gebruikers en niet-gepatchte infiltratiepunten proberen uit te buiten, maar voeren ook gefocuste aanvallen op een bepaald doel uit. De low-and-slow aanvallen zijn behoorlijke effectief geworden. Aanvallers kunnen gebruikmaken van zero-day aanvallen, hacker toolkits, social engineering-aanvallen en andere geavanceerde tactieken om detectie te voorkomen en uiteindelijk ongemerkt gegevens kan exfiltreren. In feite blijven vele aanvallen maandenlang of zelf jarenlang onopgemerkt. Zodra een bepaalde dreigingsindicator bekend is bij het grote publiek wijzigen deze geavanceerde hacker-groepen vaak hun tactiek en infrastructuur.

Dit is de reden waarom organisaties meer dan alleen maar perimeter-gebaseerde beveiliging nodig hebben. Hun mensen, technologie en processen moeten worden geïntegreerd om bedreigingen sneller te kunnen detecteren, voordat ze schade kunnen aanrichten. Bedreigingsinformatie voedt beveiligingstechnologieën en biedt de SOC (Security Operations Center) en NOC (Network Operation Center) teams de wapens om op te treden tegen relevante huidige en opkomende bedreigingen. Aan de andere kant moeten deze teams weten hoe ze deze informatie kunnen verwerken voor het beoordelen van risico's en het prioriteren van resources.

Gebruikmaken van informatie: bedreigingsinformatie kan helpen de organisatie op de hoogte te brengen van wereldwijde en branchespecifieke trends en campagnes die hen op het oog hebben en bieden inzicht naar welke waardevolle kennis de hackers op zoek zijn. Met voldoende wereldwijde informatie kunnen organisaties de aanval overnemen en op jacht naar indicatoren binnen hun omgeving. Als beslissingen worden genomen louter op basis van kennis van de activiteit binnen de omgeving van de organisatie wordt er alleen rekening gehouden met een fractie van het grote geheel. Organisaties dienen te begrijpen wat er internationaal op het gebied van bedreigingen afspeelt. Ze hebben zowel technische kennis als informatie over de vijand nodig.

Weten dat er een campagne aan de gang is die zich op een bepaalde branche richt, is slechts het begin. Organisaties dienen de details van de campagne te kennen: de persoon, de groep of het land achter de campagne, de naam van het kwaadaardige bestand dat de aanvalsgroep gebruikt, de onderwerpregels van de phishing-e-mail, de hashes en de e-mailadressen die worden gebruikt. Dit helpt organisaties bedreigingen sneller te detecteren. Dit is het type informatie waarvan het goed is dat ze met beveiligingsteams wordt gedeeld zodat zij effectiever op bedreigingen kunnen jagen.

Detecteer bedreigingen vroegtijdig: wie maakt gebruik van deze bedreigingsinformatie? Technologieën kunnen bekende bedreigingen detecteren, maar het aantal bedreigingen waarmee het gebeurtenislogboek op basis van deze technologieën wordt gevuld kan oplopen tot honderdduizenden per dag. Hoe kunnen beveiligingsteams weten welke ze moeten onderzoeken en bij welke actie vereist is? Organisaties die ernstig onder een aanval hebben geleden, realiseren zich vaak dat ze de indicatoren wel degelijk hebben gezien, maar dat er domweg te veel waarschuwingen waren om te weten wat echt cruciaal was.

Er moet een manier zijn waarop waarschuwingen worden geprioriteerd en er kan worden gefocust op de paar kritische waarschuwingen. Sommige organisaties bouwen deze mogelijkheid intern in door informatie en tal van geavanceerde technologieën te kopen en daarna een controle team, een informatieteam, een responsteam en meer aan te nemen. En omdat de hackers geen kantooruren aanhouden, dienen vooral deze controleteams 24 uur per dag en 7 dagen per week actief te zijn – en dit kan bijzonder duur zijn.

Dit is de reden waarom veel organisaties kijken of ze kunnen samenwerken met een derde partij die de mankracht en technische capaciteit van hun eigen eigen beveiligingsprogramma kan aanvullen en uitbreiden. Deze partner zou 24 uur per dag, 7 dagen per week en 365 dagen per jaar via automatische systemen en vakkundige analyse wereldwijde actieve controle moeten bieden die wereldwijde bedreigingen vergelijkt met de evenementen binnen de omgeving van de klant.

Kan proactieve controle bekende indicatoren opsporen of refereren aan historische logboekgegevens om een doelgerichte aanval te identificeren? Teams moeten in staat zijn evenementen te prioriteren binnen de omgeving – hoe kunnen ze weten wat werkelijk kritiek is?

Wanneer er vragen ontstaan, wilt u eigenlijk gewoon de telefoon oppakken en met een vertrouwd iemand spreken, alsof hij of zij binnen de muren van uw eigen bedrijf zit.

Na

Het is onvermijdelijk dat incidenten plaatsvinden en wanneer ze plaatsvinden is het zaak snel en effectief te handelen. Het doel van het responsteam is de aanval te isoleren en de schade te herstellen zodat de aanval niet resulteert in een inbreuk. Aanvallers, hoewel gedreven door verschillende motieven, proberen meestal gegevens te exfiltreren voor financieel gewin, zakelijke geheimen of concurrentievoordeel.

Ze nemen vaak ruim de tijd om dit te doen, wat betekent dat het voor organisaties die tot in de puntjes zijn voorbereid een stuk makkelijker is om een responsplan voor incidenten op effectieve wijze in werking te laten treden. Wanneer de juiste mensen zijn geïdentificeerd en aan het werk gezet, en met processen die zijn getest en reeds verder verfijnd, is de responstijd veel korter.

Wanneer een responsteam aan het werk is gezet om te onderzoeken of een mogelijke inbreuk werkelijk heeft plaatsgevonden, of om preventief actie te ondernemen tegen een bekende kritieke inbreuk, voert het team vaak discussies met hun cyberverzekeringsteam, hun juristen en vaak ook met experts van buiten om de aanval beter te begrijpen en duidelijk voor ogen te krijgen.

Zodra een incident plaatsvindt, dient het responsteam direct te reageren zonder zich zorgen te hoeven maken over de juridische en contractuele voorwaarden, zonder service level agreements uit te hoeven werken, en zonder zich door alle details over toegang en goedkeuring te hoeven worstelen. Als een organisatie zich wanneer ze van start gaat met een responsactiviteit, of tijdens de werkzaamheden, realiseert dat ze externe ondersteuning nodig heeft, is dit in dit soort noodgevallen duurder dan wanneer ze vanaf het begin een contract op afroep met een responspartner had gehad.

Zodra het plan wordt uitgevoerd en het stof is opgetrokken, is het tijd om een post-mortem uit te voeren, een afsluitende briefing van de leiding. Het is dan ook het moment om de geleerde lessen te gebruiken om het beveiligingsprogramma en het responsplan te verfijnen voor toekomstige incidenten. Wanneer dit wordt gedaan, wordt de cyclus voor het continu verbeteren van het paraatheidsprogramma gesloten.

Conclusie

Organisaties dienen verder te denken dan de perimeter en bij hun beveiligingsprogramma niet alleen te vertrouwen op technologie. Symantec kan organisaties van alle groottes en uit alle branches wereldwijd helpen tegen de geavanceerde tegenstanders van vandaag de dag te strijden. Door als het ware een verlengstuk van het beveiligingsteam van de organisatie te worden, kan Cyber Security Services organisaties helpen bij de fases voor, tijdens en na een incident en daardoor de zakelijke impact van een aanval verminderen. Zo verbeteren ze uiteindelijk de mogelijkheden van de organisatie zich voor te bereiden op een breuk en deze te voorkomen.

Om effectief te zijn, dient een beveiligingsprogramma mensen, processen en technologie te integreren.

Symantec Cyber Security Services worden zo een verlengstuk van het het beveiligingsteam van de organisatie, een service die wordt ondersteund door 500 ervaren, wereldwijd opererende professionals op het gebied van internetbeveiliging. Deze portfolio maakt het organisaties mogelijk proactief op te treden tegen opkomende bedreigingen en te voorkomen dat incidenten zich ontwikkelen tot inbreuken.

- **DeepSight™ Intelligence** volgt honderdduizenden tegenstanders over de gehele wereld voor een diepgaander begrip van moderne hackers en hun hulpmiddelen, tactieken en procedures. Organisaties hebben zowel technische als strategische informatie over tegenstanders nodig als ze opkomende bedreigingen willen kunnen voorspellen en voorkomen.
- **Managed Security Services** houdt een organisatie gefocust op kritieke bedreigingen via het wereldwijd 24/7/365 controleren op, jagen naar en analyseren van bedreigingen door een speciaal team van cyberstrijders in SOC's (Security Operation Centers) in Europa, Azië en Noord-Amerika.

- **Incident Response** biedt incidentparaatheid en activiteiten voor het ontwikkelen van responsplannen waarmee de teams worden voorbereid en processen worden opgezet voor er een incident plaatsvindt. Als er toch een aanval heeft plaatsgevonden, worden er ervaren responsteams ingezet om de bedreiging te isoleren en te vernietigen zodat incidenten zich niet ontwikkelen tot inbreuken.
- **Security Simulation** biedt een praktische, uit meerdere fasen bestaande trainingservaring die operationele kennis overbrengt van de geavanceerde aanvallen van tegenwoordig. De oefeningen zijn beschikbaar via een op de cloud gebaseerde virtuele ervaring en in de vorm van een eendaagse workshop met cursusleider ter plaatse.

Samengevat is het doel de tijd tussen de detectie en de respons te verkorten en de zakelijke impact van welke cyberbedreiging dan ook te beperken. Om een snelle en efficiënte detectie en respons mogelijk te maken, dient een organisatie ervoor te zorgen dat de beveiligingsteams en de responsprogramma's goed zijn voorbereid en paraat zijn voor een incident plaatsvindt.

Symantec kan helpen bij het ontwikkelen van de kritische operationele ervaring die noodzakelijk is om geavanceerde bedreigingen te bestrijden en werkt samen met de organisaties aan het ontwikkelen van incidentresponsprogramma's. Voor en tijdens een aanval biedt Symantec realtime controle en geavanceerde services voor het jagen op bedreigingen, services die 24/7/365 kunnen helpen bij het lokaliseren van bedreigingen, in het bijzonder wanneer analisten zijn gewapend met tijdige en relevante informatie over bedreigingen en tegenstanders. Na de aanval kan Symantec organisaties snel een nauwkeurig helpen bij het'isoleren en verminderen van een bedreiging en de operaties herstellen, zodat ze weer normaal verlopen. De lessen die uit deze activiteiten zijn getrokken, worden opgenomen in het algehele beveiligingsprogramma en gebruikt om het incidentresponsprogramma te verfijnen. Informatie over bedreigingen en tegenstanders zou een kerncomponent van het beveiligingsprogramma van elke klant moeten zijn, een component die de'beveiligingstechnologieën verrijkt en de beveiligingsteams een wapen geeft waarmee ze de risico's van'bedreigingen beter kunnen beoordelen, tegenmaatregelen kunnen implementeren en effectief actie kunnen ondernemen.

Een holistische benadering van beveiliging die mensen, technologie en wereldwijde informatie over bedreigingen integreert helpt organisaties weerbaarder te zijn tegen aanvallen en sneller over te schakelen van een louter reactieve benadering naar een proactieve benadering waarbij men opkomende bedreigingen voor is.