Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Omgaan met edge devices

Vijf uitdagingen en adviezen bij het gebruik van edge devices

10 juni 2024, versie 1.0

Introductie

Hedendaagse organisaties maken vaak gebruik van edge devices. Deze systemen bevinden zich aan de rand van het netwerk en bestaan uit (beveiligings)producten zoals firewalls, VPN-servers, routers, SMTP-servers. Terwijl dit soort edge devices bijdragen aan de productiviteit van jouw organisatie, blijkt de beveiliging van edge devices zelf regelmatig onderbelicht. Mede doordat edge devices vaak buiten het zicht vallen van moderne Endpoint Detection and Response (EDR) oplossingen. Recente incidenten bevestigen de trend dat kwaadwillenden in toenemende mate edge devices aanvallen. In dit kennisproduct gaat het NCSC dieper in op een aantal actuele uitdagingen en dreigingen bij het gebruik van edge devices en hoe organisaties hiermee om kunnen gaan.

Inleiding

Edge devices zijn niet meer weg te denken uit onze hedendaagse digitale infrastructuur. Ze vormen een essentieel onderdeel voor bijvoorbeeld veilig hybride werken (VPN-systemen) of voor het monitoren van netwerkverkeer (firewalls). Vanwege de functionaliteiten zijn edge devices meestal publiek benaderbaar via het internet en bevinden ze zich aan de rand van het netwerk. Echter kunnen ook interne systemen die publiek benaderbaar zijn via het internet worden gezien als edge device.

Recente incidenten en geïdentificeerde kwetsbaarheden binnen verschillende edge devices tonen aan dat deze producten vaak niet voldoende zijn ontworpen volgens moderne security-by-design principes. Dit terwijl deze producten wel een essentiële rol spelen bij de beveiliging van het netwerk.

Edge devices vormen al geruime tijd een aantrekkelijk doelwit voor kwaadwillenden. Statelijke actoren investeren capaciteit en middelen om onderzoek te doen en kwetsbaarheden te identificeren. Misbruik van gevonden kwetsbaarheden stelt aanvallers in staat om zich ongezien toegang te verkrijgen tot een edge device en daarmee toegang tot het achterliggende netwerk te krijgen. Een voorbeeld hiervan is het incident waarbij COATHANGER-spionagesoftware is aangetroffen op Fortigate apparaten bij het Ministerie van Defensie.[1] In het jaarverslag van de MIVD staat dat er bij deze campagne wereldwijd uiteindelijk ruim 20.000 Fortigate-apparaten zijn gecompromitteerd.[2]

Edge devices: een geliefd doelwit

Doordat vrijwel iedere organisatie één of meerdere edge devices in beheer heeft, loont het voor kwaadwillenden om technisch onderzoek te doen en naar kwetsbaarheden te zoeken binnen deze producten. De reikwijdte van gevonden kwetsbaarheden in edge devices is groot.

In het jaarverslag van 2023 beschrijft de MIVD dat Chinese actoren zich in toenemende mate richten op edge devices (specifiek VPN-systemen).[3] Echter is deze focus niet alleen beperkt tot Chinese actoren, maar bijvoorbeeld ook Russische actoren[4] en criminele ransomwaregroepen zoals Akira[5] hebben VPN-systemen misbruikt om initiële toegang te bewerkstelligen.

Doelgroep

Dit kennisproduct richt zich op personen werkzaam op tactisch niveau binnen organisaties die inzicht willen krijgen in de mogelijke risico's en dreigingen met betrekking tot edge devices binnen hun organisatie.

[1] Voor meer informatie over COATHANGER zie: https://www.ncsc.nl/actueel/nieuws/2024/februari/6/nieuwe-malware-benadrukt-aanhoudende-interesse-in-edge-devices

[2] MIVD-jaarverslag 2023: https://www.defensie.nl/downloads/jaarverslagen/2024/04/18/jaarverslag-mivd-2023

[3] MIVD-jaarverslag 2023: https://www.defensie.nl/downloads/jaarverslagen/2024/04/18/jaarverslag-mivd-2023

[4] APT44 blog van Google Mandiant: https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf

[5] CISA en NCSC-NL advisory over Akira: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a

Niet het doelwit, wel slachtoffer

Tijdens het eerste kwartaal van 2024 zijn diverse kritieke kwetsbaarheden in de VPN-oplossing Ivanti Connect Secure aan het licht gekomen. Op enkele systemen trof beveiligingsbedrijf Volexity misbruik van twee onbekende kwetsbaarheden aan, kortom zero day-kwetsbaarheden.[6]

Toen er in het openbaar over de zero day-kwetsbaarheden werd gepubliceerd, zijn de actoren over gegaan op een nieuwe strategie. Van zeer gericht misbruik van zero day-kwetsbaarheden naar grootschalig en wereldwijd misbruik van opportunistische aard. Op dat moment werd ieder kwetsbaar apparaat doelwit. Toen later ook een publieke Proof-of-Concept (PoC) code werd gepubliceerd, konden ook andere kwaadwillenden deze kwetsbaarheden misbruiken.

Deze casus is één voorbeeld van een situatie waarin iedereen slachtoffer kan worden, ondanks dat je als organisatie misschien niet het initiële doelwit bent. Enkel de aanwezigheid van een kwetsbaar systeem of product wat via het internet benaderbaar is, maakt dat een organisatie al kwetsbaar is voor opportunistisch misbruik.

Impact van een succesvolle compromittatie van een edge device

Compromittatie van een edge device biedt een kwaadwillende verschillende opties.

Zo kan een kwaadwillende besluiten om op het apparaat een backdoor te installeren om zo *persistentie* te bewerkstelligen en toegang te blijven behouden. Vaak blijven deze backdoors aanwezig na het installeren van patches en eventuele reboots. Bovendien kunnen kwaadwillenden ook de logging-functionaliteiten aanpassen waardoor het moeilijker is om verdacht gedrag te identificeren. Soms schakelen kwaadwillenden deze functionaliteiten zelfs volledig uit.

Daarnaast kan een edge device als toegangspunt voor het achterliggende netwerk worden gebruikt. Via *lateral movement* kan een kwaadwillende zich bewegen naar bijvoorbeeld een database met kritieke data of andere kroonjuwelen om deze op een later moment te exfiltreren (al dan niet via het gecompromitteerde edge device).

Tot slot verwerken edge devices vaak gevoelige gegevens zoals inloggegevens van gebruikers. Kwaadwillenden kunnen deze data exfiltreren om op een later moment terug te keren en met de inloggegevens van een medewerker op het systeem in te loggen. Het inloggen met gestolen gegevens maakt het moeilijk om onderscheid te maken tussen kwaadaardige en goedaardige activiteit op het netwerk. Dit geeft een kwaadwillende meer bewegingsvrijheid.

Gebruik van Living-off-the-Land technieken bemoeilijkt goede detectie

Bij Living-off-the-Land (LOTL)[7] maakt een kwaadwillende gebruik van legitieme tooling en applicaties in het netwerk van het slachtoffer om acties uit te voeren. Bijvoorbeeld door gebruik maken van PowerShell om kwaadaardige code uit te voeren of Active Directory-tooling om (nieuwe) inloggegevens te bemachtigen. Aangezien dit legitieme applicaties zijn worden deze veelal niet automatisch geblokkeerd, zeker wanneer ze in combinatie met valide inloggegevens worden gebruikt. Dergelijke applicaties zijn vaak aanwezig op edge devices.

Kwaadwillenden maken steeds vaker gebruik van LOTL-technieken, aangezien het een effectieve manier is om detectie te ontwijken. Bovendien bevatten edge devices vaak meerdere software libraries en applicaties die na initiële compromittatie voor verdere doeleinden gebruikt kunnen worden. Wanneer organisaties niet de juiste tooling hebben om afwijkend gedrag van legitieme applicaties te detecteren vormt dit een blinde vlek.

Monitoring en logging is complex en vaak onvoldoende geconfigureerd.

Een laatste punt dat de urgentie onderstreept is dat recente casuïstiek aantoont dat edge devices buiten de scope van traditionele EDR-oplossingen vallen. Hierdoor zijn organisaties aangewezen om zelf de logging en monitoring te configureren voor hun edge devices, waarbij er ook moet worden nagedacht over integriteitsbewaking van deze logging.

Tot op heden leert de praktijk dat het configureren van logging en monitoring op edge devices complex is en in sommige gevallen maatwerk vereist. Het kan bijvoorbeeld een uitdaging zijn om alle logging bij elkaar te brengen en te analyseren. Organisaties hebben niet altijd de capaciteit of expertise om dit uit te voeren. Bovendien zijn instructies vanuit de leverancier niet altijd toereikend of toepasbaar op eigen netwerken.

[6] Volexity blog over Ivanti Connect Secure: https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/

[7] Meer informatie over LOTL: https://www.cisa.gov/sites/default/files/2024-02/Joint-Guidance-Identifying-and-Mitigating-LOTL_V3508c.pdf

Edge devices: uitdagingen

Op basis van recente incidenten en kwetsbaarheden in edge devices en de urgentie vanuit actuele dreigingen, heeft het NCSC vijf uitdagingen gedefinieerd. Deze problemen worden daarna voorzien van handelingsperspectief om meer grip te krijgen op edge devices.

Uitdaging 1: Het aanvalsoppervlak van de organisatie is onbekend

Systemen zijn steeds meer met elkaar verbonden. Bovendien neemt de behoefte toe om op afstand en met mobiele devices te kunnen werken. Edge devices vormen vaak het koppelpunt tussen interne en externe netwerken. Wanneer de randen van het netwerk niet goed in zicht zijn en onvoldoende duidelijk is welke edge devices zich hier bevinden, vormt dit een verhoogd risico op misbruik. Systemen blijven bijvoorbeeld voor langere tijd onbedoeld kwetsbare versies draaien.

Daarnaast is het belangrijk om in kaart te brengen welke edge devices (of onderdelen ervan) via het publieke internet benaderbaar zijn. De kwetsbaarheden die op grote schaal misbruikt worden, zijn vaak op afstand en zonder interactie van een gebruiker uit te buiten. Als gevolg van dit beperkte zicht kunnen organisatierisico's onvoldoende in kaart worden gebracht. Dit maakt de rand van het netwerk een blinde vlek.

Uitdaging 2: Edge devices zijn "black boxes"

Naast het zicht op het aanvalsoppervlak, vormt onvoldoende inzicht in eigen edge devices ook een risico. Edge devices blijken lang niet altijd ontworpen volgens moderne security-by-design principes. Bovendien is het in veel gevallen complex of zelfs onmogelijk om toegang te krijgen tot de onderliggende broncode. Hierdoor is het door derden (bijvoorbeeld security experts en onderzoekers) niet mogelijk om te de veiligheid te controleren of in te zien welke softwareonderdelen aanwezig zijn.

Tijdens het misbruik van kwetsbaarheden in Ivanti Connect Secure in het eerste kwartaal van 2024 werd duidelijk dat de VPN-apparaten, softwarepakketten en libraries gebruikten van meerdere jaren oud.[8]

Veel van deze pakketten bevatten meerdere kritieke kwetsbaarheden die kwaadwillenden kunnen uitbuiten wanneer ze toegang krijgen tot een VPN-systeem.

Bovendien zijn organisaties in sommige gevallen afhankelijk van de leverancier van het edge device. In geval van Ivanti Connect Secure waren systeemlogs bijvoorbeeld niet voor gebruikers leesbaar, maar moesten de logbestanden naar de leverancier worden opgestuurd voor ontsleuteling. Daarnaast zijn software-updates vaak niet of beperkt publiek toegankelijk maar alleen beschikbaar voor klanten wat het delen van informatie bemoeilijkt. Tot slot zijn patches niet altijd tijdig beschikbaar of is de leverancier tijdens grotere incidenten onvoldoende in staat om ondersteuning te verlenen. Dit soort factoren bemoeilijkt het om een goede risico-inschatting te maken.

Uitdaging 3: Misconfiguratie van edge devices kan leiden tot een verhoogd risico op misbruik

Moderne edge devices worden steeds complexer. Waar dit soort apparaten vroeger vaak relatief eenvoudige doorgeefluiken waren van netwerkverkeer, worden nu aan edge devices steeds meer functionaliteiten toegevoegd. Alhoewel dit de gebruikerservaring ten goede kan komen, brengt dit ook nieuwe risico's met zich mee.

Sommige nieuwe functionaliteiten vereisen dat organisaties extra poorten openzetten of deze functionaliteiten via het internet toegankelijk maken. Logischerwijs biedt dit ook kansen voor aanvallers. Het gebruik van dergelijke poorten en functionaliteiten vergroot het potentiële aanvalsoppervlak, wat ook extra aandacht voor de juiste configuratie en bijbehorende monitoring en logging vereist.

Bovendien dienen extra functionaliteiten juist geconfigureerd te worden. Dit vereist capaciteit en kennis binnen de organisatie. Misconfiguratie kan er onbedoeld tot leiden dat functionaliteiten onnodig via het internet benaderbaar zijn of dat er mogelijke datalekken plaatsvinden. Dit hangt samen de voorgaande uitdagingen: de toename van functionaliteiten kan eraan bijdragen dat je verminderd zicht hebt op jouw edge devices aangezien deze ook geconfigureerd en gemonitord moeten worden. Mogelijke misconfiguraties kunnen door kwaadwillenden worden misbruikt voor het compromitteren van jouw netwerk.

[8] https://thehackernews.com/2024/02/ivanti-pulse-secure-found-using-11-year.html

Praktijkvoorbeeld uitdaging 3: SSL/TLS-offloading

Edge devices krijgen steeds meer functionaliteiten. Een voorbeeld hiervan is SSL-Offloading. Dit is een functionaliteit die gebruikers in staat stelt om verkeer, dat versleuteld is via het Secure Sockets Layer (SSL) of Transport Layer Security (TLS) protocol, te decrypten.[9] Dit helpt het edge devices om het verkeer beter te kunnen inspecteren en afwijkend verkeer te detecteren.

Wanneer een kwaadwillende zichzelf toegang tot een edge device heeft verschaft en SSL/TLS-offloading is ingeschakeld, kan dit de aanvaller toegang geven tot al het onversleutelde verkeer dat over het edge device gaat. Misbruik hiervan is een goed voorbeeld van een LOTL-techniek. Daarom is het aan te raden om het activeren en toevoegen van nieuwe functionaliteiten zoals SSL-offloading mee te nemen in een voorafgaande risicoanalyse.

Uitdaging 4: Patchmanagement voor edge devices is vaak inadequaat

Patchmanagement is een belangrijk onderdeel van ieder cybersecuritybeleid en is een van de basismaatregelen die het NCSC adviseert te treffen. [10]

Recente kwetsbaarheden in verschillende producten tonen aan dat kwaadwillenden in zeer korte tijd deze kwetsbaarheden weten te operationaliseren en op grote schaal te misbruiken.[11, 12, 13] De dreiging van dergelijk misbruik onderstreept nogmaals de urgentie van tijdig patchmanagement.

Verschillende factoren verhogen het risico op compromittatie van edge devices wanneer patchmanagement niet adequaat is:

- Patchen heeft impact op de continuïteit van organisaties. Downtime van een essentieel onderdeel zoals een VPN-systeem is tijdens kantooruren onwenselijk of zelfs onacceptabel. Daarentegen leidt uitstel van patches tot een verhoogd risico op compromittatie, zeker wanneer er publieke PoC beschikbaar is wat de kans op grootschalig misbruik vergroot.
- De urgentie van het probleem vereist dat het soms noodzakelijk is om in het weekend of de avond beveiligingsupdates te installeren op edge devices. Niet iedere organisatie heeft deze mogelijkheden.
- Service Level Agreements (SLAs) benoemen onvoldoende aan welke verplichtingen de leverancier moet voldoen op het gebied van beveiligingsupdates, communicatie hierover en ondersteuning bij het verhelpen van kwetsbaarheden. Soms zijn patches niet beschikbaar en zijn organisaties afhankelijk van mitigerende maatregelen die soms maatwerk zijn.

Uitdaging 5: Herstel na compromittatie van een edge device doet een groot beroep op de capaciteit

Het risico bestaat dat wanneer je onvoldoende bent uitgerust om dergelijke incidenten af te handelen, de impact nog veel groter is dan op het eerste gezicht lijkt. Welke data is er precies buitgemaakt? Wat is de impact op de beschikbaarheid van de systemen? Wat moeten we hierover communiceren naar klanten en partners? Wat voor invloed heeft dit op de reputatie van jouw organisatie?

In het geval van een compromittatie moeten organisaties bijvoorbeeld gebruik maken van externe, vaak kostbare, partijen die gespecialiseerd zijn in Incident Response (IR). Bovendien is het een intensief proces om de vertrouwelijkheid en integriteit van edge devices en het netwerk te herstellen. Het installeren van beveiligingsupdates of uitvoeren van een reboot is vaak onvoldoende om de toegang van een aanvaller te ontnemen en deze uit het netwerk te verwijderen. In extreme gevallen is het vervangen van de hardware de enige mogelijkheid om de integriteit van de systemen te herstellen. Naast de financiële impact vraagt dit ook veel capaciteit van de medewerkers en heeft dit consequenties voor de continuïteit van de organisatie.

Binnen het huidige dreigingslandschap is de kans aanwezig is dat iedere organisatie slachtoffer kan worden van een incident rondom edge devices. Het is daarom essentieel om de organisatie voor te bereiden op dergelijke scenario's en rekening te houden wat deze uitdagingen en risico's voor impact hebben op de continuïteit van de organisatie.

[9] Meer informatie over SSL/TLS-offloading: https://cyberpedia.reasonlabs.com/EN/ssl%20offloading.html

[10] Richt patchmanagment in: https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/beschermen/basismaatregelen-cybersecurity/richt-patchmanagement-in

[11] Beveiligingsbedrijf Mandiant beschrijft hoe meerdere actoren een kwetsbaarheid in Citrix weten te misbruiken na bekendmaking: https://www.mandiant.com/resources/blog/session-hijacking-citrix-cve-2023-4966

[12] Beveiligingsbedrijf Volexity beschrijft hoe kwaadwillenden binnen 3 dagen na publicatie van kwetsbaarheden in Ivanti Connect Secure deze op wereldwijde schaal konden misbruiken: https://www.volexity.com/blog/2024/01/15/ivanti-connect-secure-vpn-exploitation-goes-global/

[13] Blog over misbruik gericht op Palo Alto firewalls: https://www.volexity.com/blog/2024/05/15/detecting-compromise-of-cve-2024-3400-on-palo-alto-networks-globalprotect-devices/

Handelingsperspectief

Wat kun je zelf doen om de hierboven beschreven uitdaging te beheersen? Dit hoofdstuk biedt per uitdaging een aantal adviezen. Het doel hiervan is om het risico van misbruik van een edge device te inventariseren en te beheersen en de eventuele impact na misbruik te beperken.

Advies 1: Maak een overzicht van de edge devices binnen jouw organisatie en bepaal in welke mate deze via het internet benaderbaar zijn

Het kunnen beheersen van organisatierisico's als gevolg van misbruik van edge devices, begint met een overzicht van alle edge devices die jouw organisatie in gebruik heeft. Met behulp van dit overzicht krijg je niet alleen zicht op *welke* edge devices er in gebruik zijn, maar ook *waar* deze zich bevinden. Zo kun je bepalen of, en in welke mate, deze edge devices vanaf het internet benaderbaar zijn.

Je kunt dit bijvoorbeeld doen door:

- Het aanvalsoppervlak in kaart te brengen door vanaf het internet op kwetsbaarheden te scannen. Dit wordt ook wel *Attack Surface Management* (ASM) genoemd.
- In gesprek te gaan met verschillende afdelingen binnen jouw organisatie. Denk hierbij bijvoorbeeld aan SOC-medewerkers en technisch specialisten, maar ook de inkoopafdeling. Stel hierbij vragen als:
  - Welke edge devices heeft de organisatie of bestaan er plannen voor om aan te schaffen?
  - Is er een bestaand overzicht van edge devices beschikbaar?
  - Is deze up-to-date en wordt deze actief bijgehouden? En wie is hiervoor verantwoordelijk?
  - Waar bevinden edge devices zich in het netwerk? In welke mate zijn deze via het internet benaderbaar?
  - Wie configureert en beheert de edge devices?
  - Hoe worden edge devices beheerd?

Sluit, waar mogelijk, aan bij reeds bestaande asset management processen. Hierdoor vergroot je de kans dat het overzicht van edge devices ook in de toekomst wordt onderhouden.

Advies 2: Begrijp de edge devices die je in je netwerk hebt staan

Na het in kaart brengen van alle edge devices en het bijbehorende aanvalsoppervlak, bestaat de volgende stap uit inzicht krijgen in het edge device zelf. Dit biedt houvast om te bepalen welke aanvullende maatregelen op het gebied van configuratie en hardening getroffen kunnen worden. Ook geeft het inzicht in welke belangrijke afhankelijkheden er van de leverancier bestaan. Je kunt hiervoor in gesprek gaan met technische specialisten binnen je organisatie en met leveranciers.

Denk hierbij aan vragen als:

- Welke versie draait er momenteel?
- Welke functionaliteiten staan standaard ingeschakeld? Zijn er functionaliteiten die niet gebruikt worden? Zijn deze functionaliteiten vanaf het internet benaderbaar?
- Kan ik achterhalen hoe het edge device is geconfigureerd? Kunnen risicovolle functionaliteiten uitgeschakeld worden?
- Kan de leverancier bewijs aanleveren dat het edge device ontwikkeld is volgens moderne security-by-design principes?
- Kan de leverancier bewijs aanleveren dat er een onafhankelijke test (zoals een penetration test of security assessment) heeft plaatsgevonden voor het device?
- Kan de leverancier garanderen dat de software en gebruikte libraries up-to-date zijn? Kan de leverancier een Software-Bill-of-Materials (SBOM) aanleveren?
- Ben ik afhankelijk van de leverancier voor ondersteuning tijdens incidenten of kan ik zelf de benodigde informatie achterhalen en actie ondernemen? Hoe communiceert de leverancier of kwetsbaarheden en incidenten? Zijn de contactgegevens buiten kantooruren bekend?
- Waar kan de organisatie instructies vandaan halen om te configureren of beveiligingsupdates te downloaden? Voeg deze instructies toe aan een (offline) draaiboek.
- In hoeverre ben ik van de leverancier afhankelijk om tijdig te patchen?

Advies 3: Monitor edge devices

Edge devices vormen een aantrekkelijk doelwit voor kwaadwillenden. Het toepassen van actieve monitoring en detectie is daarom een belangrijke beveiligingsmaatregel om misbruik van edge devices te kunnen onderkennen. Eerder hierboven werd aangegeven dat logging en monitoring complex kunnen zijn en dat dit doorgaans maatwerk voor een organisatie vormt. Indien jouw organisatie niet over de benodigde expertise beschikt, adviseert het NCSC om de mogelijkheid voor het inhuren van externe expertise te onderzoeken.

Denk bij het inrichten van monitoring voor edge devices bijvoorbeeld aan:

- Wordt er periodiek gecontroleerd op de integriteit van configuraties (staat alles nog juist ingesteld?) en beschikbare nieuwe beveiligingsupdates?
- Wordt de logging die edge devices verzamelen naar een separate, gesegmenteerde opslag verstuurd zodat de integriteit van de logging gewaarborgd blijft?
- Wordt er actief gemonitord op verdacht gedrag op het edge device, of op de achterliggende endpoints als het niet mogelijk is om op het edge device zelf te monitoren? Om te kunnen bepalen wat afwijkend gedrag is, moet eerst worden vastgesteld wat 'normaal' gedrag is. Hiervoor kan een zogenaamde "baseline" worden ontwikkeld.

Advies 4: Besteed aandacht aan patchmanagement specifiek voor edge devices

Het is goed mogelijk dat jouw organisatie over een beleid voor patchmanagement beschikt. Vanwege de eerdergenoemde uitdagingen, adviseert het NCSC om specifiek aandacht te besteden aan patchmanagement voor edge devices. Mocht de organisatie nog niet over een beleid voor patchmanagement beschikken, dan adviseert het NCSC om dit op te stellen. Patchmanagement vormt een belangrijke basismaatregel. Onderzoek of het huidige patchmanagement voor edge devices binnen de organisatie afdoende is ingericht.

Dit kan bijvoorbeeld door te onderzoeken of:

- Er is nagedacht over wat voor jouw organisatie 'tijdig' patchen inhoudt. Dit houdt in de praktijk doorgaans verband met de impact op de continuïteit van de organisatie: zijn er bijvoorbeeld afspraken of dit binnen 24, 48 of 72 uur uitgevoerd moet worden? En wordt hier onderscheid gemaakt tussen kritieke kwetsbaarheden en reguliere updates?
- Hoe ontvangt de organisatie informatie over nieuwe kwetsbaarheden? Gebeurt dit via de leverancier of andere informatiekanalen?
- Er een besluit is genomen over mandaten en het is duidelijk wie welk mandaat heeft. Wie heeft het mandaat om te beslissen dat beveiligingsupdates toch zo snel mogelijk uitgevoerd moeten worden, ook al heeft dit impact op de activiteiten van de organisatie?
- Er voldoende capaciteit is om de beveiligingsupdates ook voor te bereiden en uit te voeren.
- Er is nagedacht over het scenario 'wat als er (nog) geen beveiligingsupdate beschikbaar is, maar er wel sprake van een kritieke kwetsbaarheid'? Wat is de aanpak in een dergelijke situatie en wat voor impact heeft dit op de organisatie?
- Is het duidelijk wat er met de leverancier van edge devices is afgesproken over patchen in een SLA? Zijn er afspraken gemaakt waar de leverancier aan moet voldoen op basis van het patchbeleid binnen jouw organisatie? Is de leverancier hier formeel mee akkoord gegaan en is de leverancier ook in staat om deze afspraken na te komen en ondersteuning te bieden conform de afspraken?

Advies 5: Beperk de impact van misbruik van edge devices voor jouw organisatie

Het is mogelijk dat jouw organisatie slachtoffer van een compromittatie van een edge device wordt. Het is in dit geval belangrijk om snel te kunnen handelen en de schade voor jouw organisatie te beperken. Door het scenario dat je slachtoffer bent geworden *(assume breach)* voor jouw organisatie uit te werken, kun je de organisatie beter voorbereiden op een incident.

Dit kan door:

- *Assume breach* als uitgangspunt te hanteren. Het wordt steeds belangrijker om over een zogeheten *defense-in-depth* beveiligingsstrategie na te denken. *Assume breach* gaat er namelijk vanuit dat de organisatie te maken krijgt met een succesvolle aanval. *Assume breach* vormt een vertrekpunt om een *defense-in-depth* beveiligingsstrategie te testen. Denk hierbij aan vragen als:
  - Leunt de organisatie momenteel op een beveiligingsmaatregel die een *single point of failure* (SPOF) blijkt te zijn als een edge device gecompromitteerd wordt?
- Zijn de omliggende netwerkinfrastructuur en -onderdelen ook ingericht volgens het *defense-in-depth* principe? Wat is bijvoorbeeld het niveau van vertrouwen en de rechten tussen deze onderdelen en edge devices? Hoe zijn netwerkonderdelen gesegmenteerd?
  - Maakt jouw organisatie zelf, of in overleg met de leverancier, gebruik van hardening voor edge devices? Leveranciers bieden vaak instructies hoe dit toe te passen.
- Het specifieke scenario van succesvol misbruik van edge devices op te nemen in je *Business Continuity Management* (BCM). Beschrijf in een *Incident Response Plan* (IRP) de eerste en belangrijkste acties die tijdens een incident genomen moeten worden.
  Voorbeelden hiervan zijn:
  - Is er nagedacht over welke kritieke processen en/of informatie als eerste veiliggesteld moeten worden en prioriteit verdienen? Is dit ook afgestemd met het bestuur van jouw organisatie?
  - Wie heeft welke mandaten, rollen, taken en verantwoordelijkheden tijdens een incident?
  - Is vastgesteld wat de maximale tijd is dat de organisatiecontinuïteit onderbroken kan worden?
  - Is voldoende capaciteit binnen de eigen organisatie aanwezig om een incident af te kunnen handelen? Of is het nodig om hier een incident response partner voor in te huren? Wat zijn de afspraken met deze partner over bereikbaarheid als er snel gehandeld moet worden? Is jouw organisatie in staat om zelf de benodigde logging aan deze partij aan te leveren? Of ben je hiervan afhankelijk van de leverancier?
    Zorg dat dergelijke afspraken met een geschikte partner al vooraf gemaakt zijn zodat er tijdens een incident niet eerst een offerte uitvraag gestart hoeft te worden.
- Tabletop-oefeningen en red teaming uit te voeren op het scenario 'compromittatie van edge devices' om de incident response plannen te simuleren, testen en verbeteren. Op deze manier kan je als organisatie beoordelen of mogelijke incident response plannen op de juiste manier in werking treden en het beoogde resultaat opleveren.

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

Juni 2024