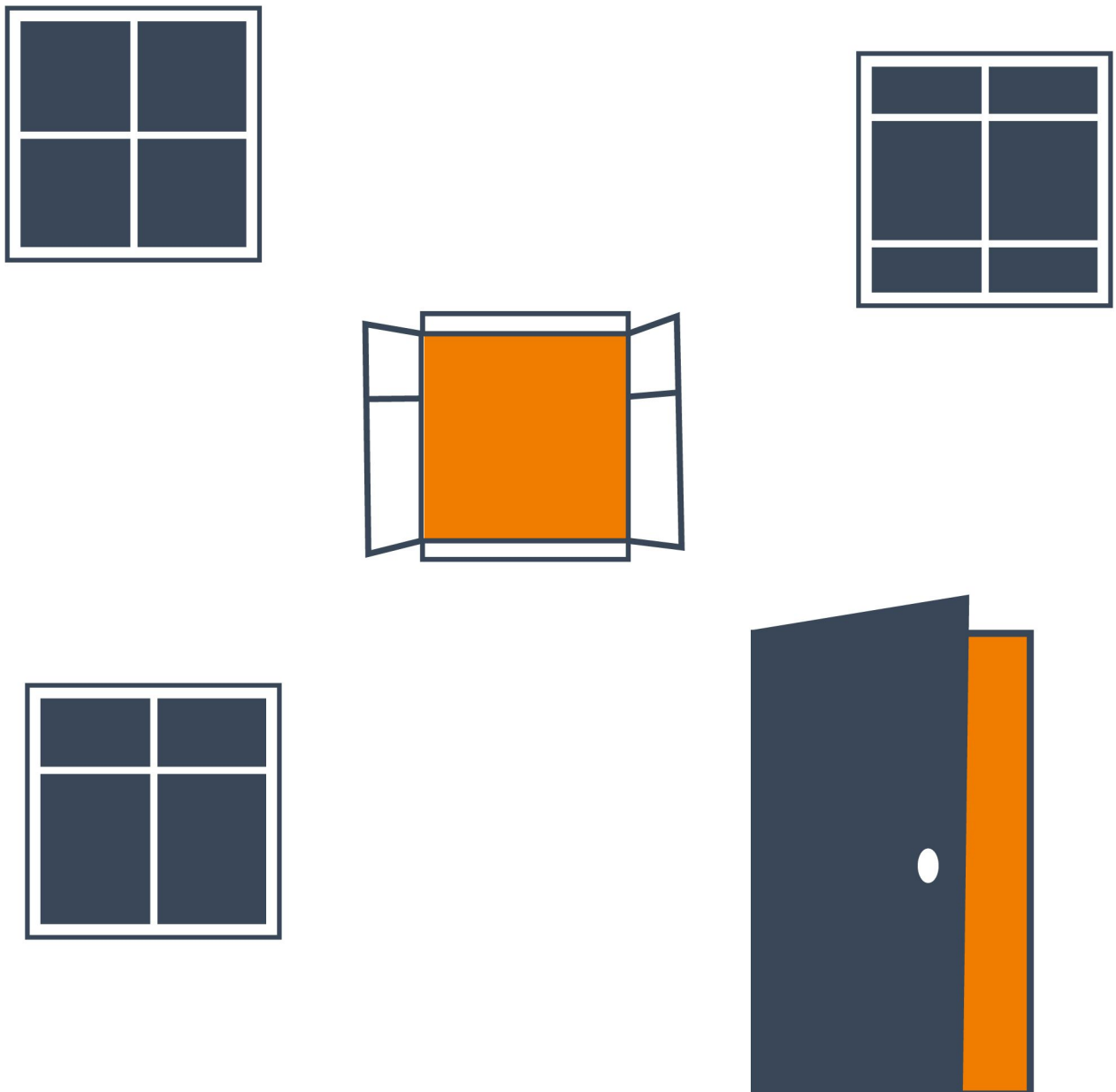
WHITEPAPER

Secquard

MSP, zijn jouw digitale ramen en deuren wel dicht?

In 5 stappen naar een verantwoordelijke security service provider



In dit **whitepaper** lees je hoe je als MSP:

- Cyberrisico's in kaart brengt
- Problemen met aansprakelijkheid voor cyberincidenten proactief oplost
- Cyberrisico's verlaagt
- Recurring revenue realiseert met cybersecurity
- Profiteert van je nieuwe status als trusted advisor op gebied van cybersecurity

Als MSP wil je natuurlijk voorkomen dat jij en je klanten slachtoffer worden van een cyberaanval. In het kader van risico's en veiligheid kun je het vandaag de dag natuurlijk ook niet meer maken om géén cybersecurity in je portfolio te hebben. Vaak zijn er tussen MSP's en klanten echter nog geen concrete afspraken gemaakt over verantwoordelijkheid bij een incident.

In dit whitepaper lees je hoe je cybersecurity onbevangen bespreekbaar maakt én hoe je je digitale ramen en deuren sluit. Zo neem je verantwoordelijkheid als dienstverlener en zorg je ervoor dat er geen problemen ontstaan op het moment dat er een cyberincident plaatsvindt. En niet geheel onbelangrijk, je realiseert er mooie terugkerende verdiensten mee..

Basismaatregelen voor cybersecurity

Hardening
Kies veilige instellingen voor al uw systemen.

Secquard controleert de status van alle veiligheidsinstellingen.

Patches & Vulnerabilities
Voer updates uit en inventariseer kwetsbaarheden

Secquard inventariseert alle updates en kwetsbaarheden.

Antivirus
Voorkom virussen en andere malware.

Secquard controleert of antivirus/ antimalware draait en of deze up-to-date is.

Autorisaties
Beperk toegang van medewerkers.

Secquard brengt de rechten van alle gebruikers in kaart.

Stap 1. Breng je grootste risico's in kaart

Meten is weten

Cyberaanvallen zijn aan de orde van de dag. We kunnen dagelijks in kranten lezen hoe steeds meer organisaties slachtoffer worden van cyberaanvallen. Zonde, want verreweg de meeste van deze aanvallen zijn zeer eenvoudig en opportuun in opzet, maar liefst 90% volgens overheidsorgaan Digital Trust Center. Dat deze simpele aanvallen toch heel succesvol zijn, komt omdat verreweg de meeste organisaties de basis van hun cybersecurity niet goed op orde hebben, veel van hun digitale ramen en deuren staan open. Het sluiten van deze digitale ramen en deuren is de beste manier om cyberweerbaar te worden. Hoe meer organisaties dit doen, hoe moeilijker het voor cybercriminelen wordt om successen te boeken. En hoe moeilijker dit wordt, hoe minder interessant deze vorm van criminaliteit wordt.

Als MSP ben je een favoriet doelwit van cybercriminelen. Je hebt namelijk een groot netwerk dat enorm aanvalsoppervlak biedt. Daarnaast hopen kwaadwillenden via dit netwerk toegang te krijgen tot jouw klanten.

Je bent extra interessant omdat de gevolgen van een cyberincident bijzonder hoog zijn: Je operatie kan tot complete stilstand komen, belangrijke data kan permanent verdwijnen, je kunt klanten verliezen en enorme reputatieschade oplopen. Je raadt het al, cybercriminelen hopen dat dit de bereidheid om snel en veel te betalen bevordert.

Wat kun je dan doen? Gelukkig zijn er een aantal eenvoudige maatregelen die je kunt treffen om deze eenvoudige aanvallen af te weren. Dit noemen wij ook wel de basismaatregelen voor cybersecurity. Deze maatregelen hebben wij niet zelf bedacht maar worden breed uitgedragen door overheden wereldwijd, zie bijvoorbeeld Digital Trust Center van onze eigen overheid. Met deze basismaatregelen ben je beschermd tegen verreweg de meeste cyberincidenten, en als er toch iets gebeurt blijft schade beperkt.

Secquard brengt in kaart in hoeverre jouw organisatie en die van je klanten de basismaatregelen hebben geïmplementeerd.

Het sluiten van de digitale ramen en deuren is de beste manier om cyberweerbaar te worden

Stap 2. Maak cybersecurity bespreekbaar

Waar je vrij van aansprakelijkheid

Nu je weet welke risico's je klant loopt, kun je deze aan de hand van een rapportage bespreken. Door je volledig op de basis van cybersecurity te richten, zijn de risico's eenvoudig toe te lichten en glashelder. Dat zijn ze ook voor mensen zonder technische achtergrond. Door de risico's aan je klant duidelijk te maken vervul je je zorgplicht als dienstverlener en expert. Je kunt de klant hierbij voorzien van een advies over het (al dan niet) aanpakken van deze risico's.

Je kunt direct van deze gelegenheid gebruikmaken om je klant eraan te herinneren (of erover te informeren) dat deze zelf verantwoordelijkheid draagt voor haar cyberrisico. Klanten van MSP's denken namelijk nog wel eens – ten onrechte – dat de verantwoordelijkheid voor een cyberincident compleet bij de dienstverlener ligt. Door hier duidelijkheid over te scheppen, zorg je ervoor dat er geen extra vervelende situaties ontstaan als er toch onverhoopt een cyberincident plaatsvindt.

Bespreek de risico's aan de hand van rapportages

Stap 3. Maak een plan voor het verlagen van de risico's

Stel een actieplan op

Nu de klant zich bewust is van haar belangrijkste cyberrisico's en haar eigen verantwoordelijkheid op het gebied van cybersecurity, is het belangrijk om samen met de klant te bepalen hoe een veilige omgeving voor deze klant er dan precies uit ziet. Hierbij maak je samen een afweging tussen verwachte inspanning/kosten en verlaging van risico's. Het zal je niet verbazen dat de ene klant wat veeleisender in is dan de andere. Maar, in de praktijk zien wij eigenlijk altijd dat internationaal geaccepteerde best practices in eerste instantie meer dan voldoen om uw klant te helpen naar een veiligere omgeving.

Door in het plan vast te houden aan de basismaatregelen, houd je het begrijpelijk voor alle partijen.
Secquard heeft hiervoor complete documentatie beschikbaar zodat je hier zelf niets voor hoeft uit te zoeken, je loopt gewoon samen met de klant een document door. Dit zorgt ervoor dat je met de klant, binnen een paar uurtjes het hele plan hebt gemaakt. Daarnaast zijn de best practices voor de basismaatregelen met relatief weinig inspanning te realiseren. Dat helpt om de kosten laag te houden terwijl je veel voortgang boekt op gebied van cyberveiligheid.

Bepaal hoe een veilige omgeving er precies uitziet

Stap 4. Voer het plan uit

Verlaag risico's

Nu de klant de risico's kent, zich realiseert dat zij verantwoordelijkheid draagt voor cyberrisico én weet wat er moet gebeuren om cyberweerbaar te worden, kan zij beslissen wie de werkzaamheden uit gaat voeren. De basismaatregelen zijn namelijk eenvoudig en kunnen indien gewenst door de klant zelf uitgevoerd worden. Dat je de klant deze keuze biedt schept vertrouwen, je komt immers niet zomaar wat verkopen, maar helpt de klant om veiliger te worden. In de realiteit zien wij echter dat de klant vaak geen capaciteit of ambitie heeft om de verbeterstappen zelf op te pakken. Hier ligt voor jou als MSP een volgend verdienmodel.

Voor het doorvoeren van verbeter-werkzaamheden reken je een uurtarief maal het aantal uren dat je spendeert. Hierin moeten natuurlijk een aantal belangrijke keuzes worden gemaakt. Zoals de snelheid waarmee de klant graag wil dat de verbeteringen worden doorgevoerd en de frequentie waarmee u samen de voortgang bespreekt. Vaak ligt de frequentie op eens per maand. Je gebruikt hiervoor eenvoudig de Secquard rapportage, die in één oogopslag laat zien in hoeverre de verbeteringen zijn doorgevoerd. Mocht het nodig zijn dan kun je er samen voor kiezen om werkzaamheden te versnellen.

Verdienmodel MSP:
Recurring revenue centraal

- Maandelijks leveren van rapportages
- Opstellen cybersecuritybeleid
- Uitvoering geven aan beleid

Stap 5. Profiteer van de versterkte relaties met uw klanten

Pluk de vruchten

Hoewel het voor jou als MSP wat lastig kan zijn om naar je klant toe te stappen met het verhaal dat hun systemen niet helemaal veilig zijn, merken wij bij onze huidige partners dat klanten deze eerlijkheid juist erg waarderen.

Doordat je proactief naar de klant gaat met een extern rapport van Secquard en laat zien wat de belangrijkste cyberrisico's zijn, weet de klant precies waar zij aan toe is. Door het probleem niet alleen aan te kaarten, maar ook nog eens een betaalbare oplossing te bieden die snel gerealiseerd kan worden en werkt volgens principes die door bijvoorbeeld het Digital Trust Center worden ondersteund, ziet de klant jou nu – terecht – als trusted advisor op gebied van cybersecurity. Wanneer de klant de basis van cybersecurity op orde heeft, kun je, indien gewenst, additionele cybersecurityproducten en -diensten verkopen om de organisatie nog veiliger te maken. Wij adviseren om de Secquard rapportages maandelijks aan klant te blijven leveren, zo staan jullie beiden nooit voor verrassingen.

Wees een trusted advisor op gebied van cybersecurity

Voordelen voor jou als MSP

- Verlaag uw risico's en die van uw klanten
- Werkwijze ondersteund door overheid (DTC)
- Voorkom verwijten en aansprakelijkheid in geval van een cyberincident
- Versterk relaties met klant, word trusted advisor
- Perfecte basis voor cybersecurity portfolio en het leveren van aanvullende cybersecurityproducten en diensten
- Supersnel geïmplementeerd
- Recurring revenue
- Volledige ondersteuning vanuit Secquard voor marketing, sales en implementatie.

Secquard

Hoofdadres:
Pikeursbaan 12
7411 GV Deventer

Bezoekadres:
Wilhelmina van Pruisenweg 104
2595 AN Den Haag

info@secquard.com