

24/7 Emergency Response bij Hacking

Secutec's SecureRESPONSE Team, ons eigen toegewijde Cybersecurity Incident Response Team of CSIRT, ondersteunt organisaties om efficiënt te reageren op cybersecurity incidenten om de schade veroorzaakt door aanvallers te minimaliseren. Het biedt een raamwerk waarmee we de omvang en het risico van het incident bepalen, de dreiging indammen, adequaat en snel reageren op dat incident, communiceren over de resultaten en risico's aan alle belanghebbenden en de kans verkleinen dat een incident zich opnieuw voordoet.

Ons team is **24/7** beschikbaar en neemt het voortouw in het begeleiden van zowel uw eigen IT-team als eventuele IT-partners tijdens de duur van het project. In samenwerking met het management van het bedrijf **definiëren we verschillende scenario's voor het herstellen van de operationele status van uw digitale omgeving**, waarbij we rekening houden met de beveiligingsrisico's en financiële impact. Uiteindelijk beslist u welk scenario het beste aansluit bij uw behoeften.

We hebben ruime ervaring in het omgaan met verschillende soorten beveiligingslekken en hebben **ransomware-onderhandelingen gevoerd voor vooraanstaande instellingen** in verschillende landen over de hele wereld.

Verhoog uw zekerheid met SecureCARE

Nog steeds zijn te weinig bedrijven goed voorbereid op cyberincidenten en -aanvallen. **Het resultaat?** Aanzienlijke economische schade, reputatieverlies, het lekken van waardevolle gegevens, het stilvallen van activiteiten of in het ergste geval het einde van uw bedrijf.

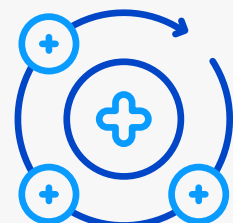
Door u te abonneren op SecureCARE, onze SecureRESPONSE SLA, krijgt u toegang tot een van de meest onschatbare voorzieningen ter wereld: **gemoedsrust**. Met deze Service Level Agreement activeert ons toegewijde Incident Response Team de incident response service binnen 4 uur na uw eerste telefoontje.



**24/7
ONDERSTEUNING**



**GEEN EXTRA
KOSTEN**



**EFFECTIEVE
REACTIE**

Incident Response Lifecycle

De Incident Response Lifecycle-benadering garandeert een gestructureerde methodologie voor het omgaan met inbreuken op de beveiliging en schetst de belangrijkste fasen voor een snelle en uitgebreide respons en herstel.

FORENSISCHE ANALYSE EN ONDERZOEK | DE KRACHT VAN THREAT INTELLIGENCE

Het SecureRESPONSE-team komt onmiddellijk in actie om de **bedreiging in te dijken** en de **verspreiding te beperken** om verdere schade te voorkomen en de bedreiging uit de omgeving te verwijderen. In deze fase onderzoeken we ook de **hoofdoorzaak van de aanval**, hoe deze uw systemen is binnengekomen en hoe ver deze zich - intern en mogelijk extern - heeft verspreid.

Tijdens de onderzoeks- en analysefase combineren we **threat intelligence-technologie** zoals XDR en forensische tools met onze eigen Secutec SecureDNS-verdedigingsmaatregelen. Met behulp van de informatie over bedreigingsactoren, aanvalspatronen en -technieken **beoordelen we de ernst van de bedreiging en de potentiële impact** op de organisatie en doen we een **eerste voorstel voor de herstel- en heropbouwopties**.

HERSTEL | "TO PAY OR NOT TO PAY"

Op basis van de uitkomst van de analyse en de geïdentificeerde herstelopties spelen we een adviserende rol bij de belangrijke beslissing om al dan niet te betalen om de versleutelde gegevens te ontgrendelen. Als deze keuze wordt gemaakt, of om alle mogelijkheden open te houden, neemt ons team het initiatief om contact op te nemen met de hacker, en worden de **onderhandelingen** gestart na goedkeuring van de CEO.

INTERNE & EXTERNE COMMUNICATIE | HERSTEL HET VERTROUWEN

Intelligente communicatie is de sleutel tot vertrouwenherstel, zowel naar medewerkers als naar externe belanghebbenden. Secutec ondersteunt u door elke actie te documenteren en een **compleet en uitgebreid rapport van het incident** aan de CEO van uw bedrijf aan te leveren. Wij helpen uw interne IT-team of externe partner met alle interne communicatie. Daarnaast assisteren we bij het **rapporteren aan de relevante autoriteiten**.

Herbouw een veilige omgeving

Ons SecureRESPONSE-team werkt naadloos samen met uw aangewezen IT-afdeling of IT-partner van uw voorkeur om robuuste beveiligingsprogramma's en -processen te implementeren om verdere schade aan uw digitale infrastructuur te voorkomen.

- **Beveiligingsbeleid:**

We werken actief samen met uw team aan de ontwikkeling en handhaving van het benodigde beveiligingsbeleid om de algehele beveiliging van uw digitale omgeving te verbeteren.

- **Adviesdiensten:**

Op basis van onze uitgebreide kennis en ervaring biedt ons team aanbevelingen op maat en strategische inzichten om de effectiviteit van uw beschermende maatregelen te maximaliseren.



E-book

Voorkomen is beter dan genezen

Hoe kunnen we het risico van een cyberaanval op uw organisatie minimaliseren? Laten we gezamenlijk de meest passende maatregelen bekijken. Moeten we het personeel bewust maken door middel van training? Misschien is een grondige beveiligingsaudit noodzakelijk, of is voortdurende monitoring cruciaal? Als u de stress en kosten wilt verminderen, aarzel dan niet om contact met ons op te nemen. We kunnen dan de op maat gemaakte oplossingen bespreken die we voor uw organisatie kunnen bieden.

Meer weten?

Neem **contact** met ons op of **download** het E-book 'Emergency Response To Hackers'.