

24/7-Notfallreaktion auf Hackerangriffe

Das SecureRESPONSE-Team von Secutec, unser eigenes dediziertes Cybersecurity Incident Response Team oder CSIRT, unterstützt Organisationen dabei, effizient auf Cybersecurity-Vorfälle zu reagieren, um die durch Angreifer verursachten Schäden zu minimieren. Es bietet einen Rahmen, mit dem wir den Umfang und das Risiko des Vorfalls bestimmen, die Bedrohung eindämmen, angemessen und schnell auf diesen Vorfall reagieren, über die Ergebnisse und Risiken an alle Interessengruppen kommunizieren und die Wahrscheinlichkeit eines erneuten Auftretens eines Vorfalls verringern.

Unser Team ist **24/7** verfügbar und übernimmt die Führung bei der Beratung sowohl Ihres eigenen IT-Teams als auch möglicher IT-Partner während der gesamten Projektdauer. In Zusammenarbeit mit der Unternehmensleitung werden **verschiedene Szenarien zur Wiederherstellung des operativen Status Ihrer digitalen Umgebung definiert**, wobei Sicherheitsrisiken und finanzielle Auswirkungen berücksichtigt werden. Letztendlich können Sie die Entscheidung über das Szenario treffen, das am besten Ihren Bedürfnissen entspricht.

Wir verfügen über umfangreiche Erfahrungen im Umgang mit verschiedenen Arten von Sicherheitsverletzungen und haben die **Verhandlungen über Lösegeldzahlungen für äußerst wichtige Institutionen** in verschiedenen Ländern weltweit geleitet.

Steigern Sie Ihre Sicherheit mit SecureCARE

Noch immer sind zu wenige Unternehmen angemessen auf Cyber-Vorfälle und Angriffe vorbereitet. **Das Ergebnis?** Schäden in Höhe von Zehntausenden Euro oder mehr, Rufschädigung, der Verlust wertvoller Daten, die Stilllegung Ihres Unternehmens.

Durch den Abschluss eines Abonnements für SecureCARE, unser SecureRESPONSE SLA, erhalten Sie Zugang zu einem der wertvollsten Güter der Welt: **innerer Ruhe**. Durch diesen Service-Level-Vertrag aktiviert unser engagiertes **Incident-Response-Team** den Incident-Response-Service **innerhalb von 4 Stunden** nach Ihrem ersten Anruf.



**24/7
UNTERSTÜTZUNG**



**KEINE
VERSTECKTEN
KOSTEN**



**EFFEKTIVE
REAKTION**

Incident Response Lifecycle

Der Ansatz des Incident-Response-Lebenszyklus garantiert eine strukturierte Methodik zur Behandlung von Sicherheitsverletzungen und skizziert Schlüsselphasen hin zu einer schnellen und umfassenden Reaktion und Wiederherstellung.

FORENSISCHE ANALYSE & UNTERSUCHUNG | NUTZUNG DER LEISTUNG VON BEDROHUNGS-AUFLÄRUNG

Das SecureRESPONSE-Team handelt sofort, um **die Bedrohung einzudämmen** und die Ausbreitung zu begrenzen, um weitere Schäden zu verhindern und die Bedrohung aus der Umgebung zu entfernen. In diesem Stadium untersuchen wir auch **die Ursache des Angriffs**, wie er in Ihre Systeme gelangt ist und wie weit er sich - intern und potenziell extern - verbreitet hat.

Während der Untersuchungs- und Analysephase kombinieren wir **Bedrohungsaufklärungstechnologien** wie XDR und forensische Tools mit unseren eigenen defensiven Maßnahmen von Secutec SecureDNS. Basierend auf Informationen über Angreifer, Angriffsmuster und -techniken bewerten wir **die Heftigkeit der Bedrohung und ihre potenziellen Auswirkungen** auf die Organisation und machen **einen ersten Vorschlag für die Wiederherstellungs- und Wiederaufbauoptionen**.

WIEDERHERSTELLUNG | "ZAHLEN ODER NICHT ZAHLEN"

Basierend auf den Ergebnissen der Analyse und den identifizierten Wiederherstellungsoptionen spielen wir eine beratende Rolle bei der wichtigen Entscheidung, ob gezahlt werden soll oder nicht, um die verschlüsselten Daten freizuschalten. Wenn diese Entscheidung getroffen wird oder um alle Optionen offen zu halten, übernimmt unser Team die Führung bei der Kontaktaufnahme mit dem Hacker und beginnt nach Genehmigung des CEOs mit **den Verhandlungen**.

INTERNE & EXTERNE KOMMUNIKATION | DAS VERTRAUEN WIEDERHERSTELLEN

Intelligente Kommunikation ist der Schlüssel zur Wiederherstellung des Vertrauens, sowohl gegenüber Mitarbeitern als auch externen Stakeholdern. Secutec unterstützt Sie durch Dokumentation jeder Aktion und **Erstellung eines vollständigen und umfassenden Berichts über den Vorfall** für den CEO Ihres Unternehmens. Wir unterstützen Ihr internes IT-Team oder Ihren externen Partner bei aller internen Kommunikation. Darüber hinaus helfen wir bei **der Berichterstattung an die relevanten Behörden**.

Eine sichere Umgebung wiederherstellen

Unser SecureRESPONSE-Team arbeitet nahtlos mit Ihrer festgelegten IT-Abteilung oder Ihrem bevorzugten IT-Partner zusammen, um robuste Sicherheitstools und -prozesse umzusetzen, die darauf abzielen, weitere Schäden an Ihrer digitalen Infrastruktur zu verhindern.

- **Sicherheitsrichtlinien:**

Wir arbeiten aktiv mit Ihrem Team zusammen, um benötigte Sicherheitsrichtlinien zu entwickeln und durchzusetzen, die darauf abzielen, die allgemeine Sicherheitslage Ihrer digitalen Umgebung zu verbessern.

- **Beratungsdienste:**

Basierend auf unserem umfangreichen Wissen und unserer Erfahrung bietet unser Team maßgeschneiderte Empfehlungen und strategische Einblicke, um die Wirksamkeit Ihrer Schutzmaßnahmen zu maximieren.



E-book

Vorbeugen ist besser als heilen

Wie können wir das Risiko eines Cyberangriffs auf Ihr Unternehmen minimieren? Lassen Sie uns zusammenkommen, um die geeignetsten Maßnahmen zu erkunden. Könnte es sein, dass die Sensibilisierung der Mitarbeiter durch Schulungen verbessert wird? Vielleicht ist eine umfassende Sicherheitsüberprüfung angebracht, oder vielleicht ist eine kontinuierliche Überwachung der Schlüssel? Wenn Sie darauf bedacht sind, Stress und Kosten zu reduzieren, kontaktieren Sie uns, und wir können über die maßgeschneiderten Lösungen sprechen, die wir für Ihr Unternehmen anbieten können.

Kontaktieren Sie uns oder laden Sie das E-Book "Emergency Response To Hackers"