TRUESEC

Produktblatt

Cybersecurity Incident Response

Zunehmende Cyberbedrohungen erfordern professionelle Abwehrkapazitäten

Predict Prevent Detect **Respond** Recover

Wirtschaftsunternehmen, Energieversorger, Bildungs- und Gesundheitseinrichtungen, ganze Landkreise: In unserer zunehmend vernetzten Welt wächst die Bedrohung durch Cyberangriffe rasant, und sie richtet sich gegen sämtliche Bereiche unserer Gesellschaft. Cyberkriminelle werden immer besser darin, Schwachstellen von IT-Systemen zu finden und passen ihre Angriffsmethoden laufend an.

Die Verschlüsselung von IT-Systemen durch Ransomwareattacken kann Unternehmen schnell in Existenznot bringen; der Diebstahl vertraulicher Firmeninformationen oder Kundendaten die Unternehmensreputation nachhaltig schädigen. Angriffe auf staatliche Institutionen und kritische Infrastruktur bergen das Risiko weitreichender Bedrohungen und Schäden für unsere Gesellschaft und die öffentliche Sicherheit.

Sie vermuten die Kompromittierung Ihrer Betriebssysteme oder sehen Ihre Organisation einem Cyberangriff ausgesetzt? Verlieren Sie keine wertvolle Zeit! Unser dediziertes und hochperformantes Incident Response Team steht jederzeit für Sie bereit. Unsere Expert:innen sorgen für die entschiedene Umsetzung aller, für die Abwehr des Angriffs und die schnelle Wiederherstellung Ihrer Betriebsfähigkeit, notwendigen Maßnahmen.

Was tun bei einem Cyberangriff?

1. Ruhe bewahren!
2. Kontaktieren Sie Truesec und fordern Sie professionelle Hilfe an!
3. Schalten Sie nichts ab!
4. Sichern Sie Ihre Backups - offline!
5. Protokollieren Sie die Abfolge der Ereignisse.

(Lesen Sie mehr hierzu auf S. 4)

Über uns

Als globales Cybersicherheitsunternehmen stehen wir im Kampf gegen Cyberkriminalität an vorderster Front und schützen nicht nur Organisationen, sondern die ganze Gesellschaft. Seit unseren Anfängen haben wir eine klare Mission: Cyberangriffe verhindern und ihre Auswirkungen begrenzen, um die digitale Welt sicherer und nachhaltiger zu machen. Wir erfinden uns ständig neu und arbeiten Tag für Tag daran, unsere Kapazitäten zum Schutz Ihrer Daten und Systeme zu optimieren.

TRUESEC

A Safe Digital Future

Kontaktieren Sie uns

+49 (0) 89 380 30 900
germany@truesec.com
de.truesec.com

Das Truesec CSIRT unterstützt Sie schnell und professionell

Wir stehen Ihnen im Falle eines Cyberangriffs zur Seite.

Truesec CSIRT: Wir retten Daten, Systeme und ganze Organisationen

Das Truesec Cyber Security Incident Response Team (CSIRT) verfügt über langjährige und profunde Erfahrung in der Bekämpfung von Cyberkriminalität auf der ganzen Welt. Zu unseren Einsatzgebieten gehören komplexe Ransomware-Kampagnen, Cyberspionage und der Diebstahl digitaler Vermögenswerte. Von der Bekämpfung von Cyberangriffen über forensische Analysen bis zur Wiederherstellung betriebskritischer Systeme: Unsere Expert:innen stoppen Cyberkriminelle entschlossen und effektiv. Unser Knowhow in Kombination mit den fortschrittlichsten Tools versetzen uns in die Lage, Bedrohungen und Angriffe schnell und entschieden abzuwehren und Systeme und Daten zu retten.

Schnelligkeit

Die Auswirkungen einer komplexen Cyberattacke sind oftmals verheerend. Die Kosten für Betriebsunterbrechungen können für Unternehmen schnell existenzgefährdend sein. Angriffe auf kritische Infrastruktur können die öffentliche Ordnung und Sicherheit erheblich bedrohen.

Die entschiedene Abwehr und Eindämmung von Cyberangriffen ist daher essenziell, und dank unserer Praxiserfahrung können wir von komplexen Cyberangriffen betroffenen Organisationen schnell und effektiv helfen. **So können wir die betriebskritischen Systeme unserer, von komplexen Ransomwareangriffen betroffenen Kunden in über 90 Prozent der Fälle in weniger als sieben Tagen wiederherstellen.**

Unser hochperformantes CSIRT besteht aus:

- IT-Forensikern
- Threat Intelligence Expert:innen
- Recovery-Expert:innen
- Reverse-Engineering-Spezialist:innen
- Incident Managern
- Rechtsexpert:innen und
- Krisenmanagern

TRUESEC

A Safe Digital Future

Kontaktieren Sie uns

+49 (0) 89 380 30 900
germany@truesec.com
de.truesec.com

Unser bewährter Incident Response-Ansatz

Sieben Schritte definieren unsere Vorgehensweise.

Der Incident Response Prozess

Das Truesec CSIRT verfolgt einen bewährten, klar definierten Prozess in enger Zusammenarbeit mit den Vertretern Ihrer Organisation. Für einen schnellen und sicheren Ablauf wird die Arbeit in mehrere Workstreams mit spezialisierten Fachkräften aufgeteilt.

1. Kontaktaufnahme und Startbesprechung

Truesecs Incident Response-Manager verschafft sich in Zusammenarbeit mit Ihrer IT einen Überblick über die Art des Vorfalls sowie das Ausmaß des Schadens und entwickelt einen Handlungsplan. Wir unterstützen Sie zudem bei der Einrichtung alternativer Kommunikationskanäle, da Ihr Mailsystem in der Regel kompromittiert sein wird.

2. Vorbereitung

Die Nachforschungen beginnen mit der Sammlung sämtlicher Informationen, die für die Erstellung eines Lagebildes und spätere forensische Analysen notwendig sind. Die Beschaffung sachdienlicher Informationen erfolgt sowohl durch das Sammeln von Daten aus Ihren Systemen als auch mittels Interviews mit Experten Ihrer Organisation.

3. Eindämmung

Im Rahmen des Eindämmungsworkflows stellen wir die Begrenzung des Schadens sicher. Das Truesec Security Operation Center (SOC) aktiviert eine Sicherheitsüberwachung Ihrer Systeme, um einen vollumfänglichen Überblick über Ihr IT-Milieu zu erlangen. Dies ist insbesondere dann wichtig, wenn der Angreifer in Ihre Umgebung vorzudringen oder sich darin zu bewegen versucht.

4. Forensische Analysen und Ermittlungen

Es erfolgt eine gründliche forensische Untersuchung zu den Aktivitäten der Angreifer innerhalb Ihres IT-Milieus. Neben der Sicherung potenziell wichtiger Spuren wird untersucht, ob firmen- oder personenbezogene Daten exfiltriert oder offengelegt wurden. Ferner ermitteln wir im Detail, wie sich die Angreifer Zugang zu Ihrem System verschaffen konnten. Mittels Nachforschungen in Dark Web-Quellen führen wir außerdem eine detaillierte Bedrohungsanalyse der Angreifer durch.

5. Beseitigung

Auf Grundlage der Ergebnisse der forensischen Untersuchung werden präzise und effektive Maßnahmen ergriffen, um den Angreifer vollständig und dauerhaft aus Ihrem IT-Milieu zu entfernen. Hierbei werden sämtliche mit dem Angreifer zusammenhängende Artefakte beseitigt und somit der ursprüngliche Zustand Ihres IT-Milieus sichergestellt.

6. Wiederherstellung

Sofern möglich erfolgt schließlich die sichere Wiederherstellung der operativen Kapazitäten Ihres IT-Milieus. Bei Bedarf helfen wir Ihnen beim Neuaufbau von nicht wiederherstellbaren Systemen.

7. Abschlussbericht und Nachbereitung

Nach erfolgreichem Abschluss des Incident Reponse-Prozesses und der Wiederherstellung Ihrer Betriebsfähigkeit verfasst das Truesec CSIRT einen Fallbericht und stellt sicher, dass Ihre operativen Abläufe und Incident-Response-Pläne mit Hilfe der gewonnenen Erkenntnisse ergänzt werden. Truesec bietet zudem die weitere, aktive Sicherheitsüberwachung Ihrer Systeme für einen vereinbarten Zeitraum an, um eine reibungslose Rückkehr zum Normalbetrieb zu gewährleisten.

Kontaktieren Sie uns

+49 (0) 89 380 30 900
germany@truesec.com
de.truesec.com

Sie vermuten einen Cybernotfall? Kontaktieren Sie das Truesec CSIRT!

+49 (0) 89 380 30 900
incident@truesec.com

Leistungsumfang Incident Response	Inklusive	Optional
Truesecs bewährte Cyber Incident Response-Methodik	✓	
Analyse durch die Truesec Threat Intelligence-Einheit	✓	
Truesecs proprietäre Threat Intelligence-Plattform	✓	
Recovery aller wiederherstellbaren Daten aus verschlüsselten Dateien	✓	
Abschlussbericht und Nachbereitung	✓	
Aktive Sicherheitsüberwachung durch das Truesec Security Operations Center (SOC) während des Incident Response-Prozesses		✓
Aktive Sicherheitsüberwachung durch das Truesec SOC nach Abschluss des Incident Response-Prozesses (üblicherweise drei bis sechs Monate)		✓
Krisen- und Kommunikationsmanagement		✓
Neuaufbau nicht wiederherstellbarer Systeme		✓

Verhalten im Fall eines Cyberangriffs

1. Bewahren Sie Ruhe!

Die folgenden Regeln helfen Ihnen, besonnen zu handeln und so den Schaden zu begrenzen.

2. Kontaktieren Sie Truesec!

Sichern Sie sich die Unterstützung durch erfahrene Cybersecurity-Profis. Sehen Sie von eigenen Maßnahmen ab, bis die IT-Sicherheitsexperten mit der Untersuchung beginnen, um einen Verlust forensischer Daten zu vermeiden.

3. Schalten Sie nichts ab!

Vermeiden Sie es, Computer auszuschalten, Stecker herauszuziehen, Konten zu deaktivieren oder sonstige Änderungen an Ihren IT-Systemen vorzunehmen. Betrachten Sie Ihr IT-Milieu wie einen Tatort.

4. Sichern Sie Ihre Backups – offline!

Sichern Sie Ihre Backups so, dass sie sich nicht in einem Netzwerk befinden. Kritische Systeme können vom Netzwerk getrennt werden – aber schalten Sie diese bitte nicht aus!

5. Dokumentieren Sie sämtliche Ereignisse!

Protokollieren Sie, wie Sie den Vorfall erlebt haben, indem Sie die fünf W-Fragen beantworten: Wer, was, wann, wo und warum. Hierbei zählt jedes Detail.

Kontaktieren Sie uns

+49 (0) 89 380 30 900
germany@truesec.com
de.truesec.com