RANSOMWARE

Technische Schwachstellen und fehlende organisatorische Kontrollen in der IT können Angreifern die Tore zu Ihrem Unternehmen öffnen. Deshalb sollten Sie jetzt moderne Standards und Sicherheitsrichtlinien etablieren, um sich effektiv vor Cyberangriffen zu schützen.

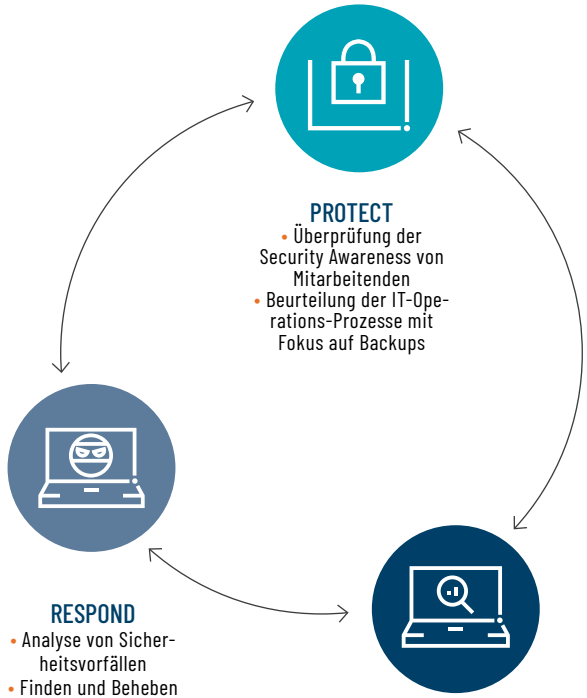
Angreifer nutzen menschliche Schwäche

Bei Ransomware-Angriffen werden Unternehmensdaten verschlüsselt und erst nach Zahlung eines „Lösegelds“ wieder nutzbar gemacht. Als typischer Angriffsvektor kommt Social Engineering zum Einsatz. Beispielsweise wird Schadsoftware als E-Mail-Anhang versendet, über die bei Ausführung Unternehmensdaten verschlüsselt werden.
Angreifer nutzen also nicht mehr nur technische Sicherheitslücken in IT-Systemen aus, sondern machen sich zunehmend menschliche Schwächen zunutze – mit den einfachsten Mitteln. In der jüngsten Vergangenheit verbuchten so auch deutsche Unternehmen Schäden in Milliardenhöhe.

Schnelles Handeln ist entscheidend

Wenn ein Ransomware-Befall erkannt wurde, müssen Unternehmen so schnell wie möglich reagieren, um die Auswirkungen gering zu halten. Wichtig ist vor allem die Isolation von betroffenen Systemen, damit sich die Ransomware nicht weiter im internen Netzwerk verbreiten kann. Es sollte außerdem geprüft werden, ob Backups vorhanden sind, um die Geschäftstätigkeit fortsetzen zu können.

Unsere Strategie gegen Ransomware-Attacken



protiviti®
Global Business Consulting

85+ Standorte | **25** Länder | **9000+** Mitarbeitende

Protiviti berät Unternehmen praxisorientiert und auf Augenhöhe in den Bereichen Strategie, Organisationstransformation und -optimierung, ESG, Digitale Transformation, Risikomanagement, Interne Revision und Kontrollsysteme, Compliance sowie IT. Gemeinsam finden wir individuelle Lösungsansätze, um Ihr Unternehmen zukunftssicher aufzustellen.
Face the Future with Confidence.

Schnell handeln, Schaden begrenzen: Ihr Ransomware-Notfallplan

1 **Identifizierung und Isolation** der befallenen Systeme
2 **Analyse der Aktivitäten** des Angreifers
3 **Prüfung:** Sind Backups vorhanden, die wiederhergestellt werden können?
4 **Ermittlung:** Ist der Vorfall anzeigepflichtig?
5 **Einleitung und Verbesserung** der Gegenmaßnahmen

Mit Protiviti stark gegen Cyberangriffe

Wir helfen Unternehmen, sich vor Ransomware-Angriffen zu schützen, auf diese zu reagieren und die bestmöglichen Entscheidungen zu treffen. Mithilfe automatisierter und manueller Analysen überprüfen wir Ihre kritische Infrastruktur auf potenzielle Eintrittspunkte für Ransomware, die Angreifer ausnutzen könnten.
Unsere Fachleute sind explizit auf die Beratung in Bezug auf Ransomware spezialisiert. Sie stehen Ihnen zur Seite, wenn es darum geht, die richtigen Entscheidungen im Umgang mit Ransomware zu treffen. Wir unterstützen Sie bei der Bewertung Ihrer Optionen, einschließlich der Frage, ob Verhandlungen mit den Angreifern eine sinnvolle Strategie sind. Protiviti hilft Ihnen dabei, Ihr Unternehmen vor Ransomware zu schützen und sicherzustellen, dass Sie im Falle eines Angriffs die richtigen Entscheidungen treffen.

UNSERE SERVICES

- RISIKO- UND BEDROHUNGSANALYSEN
- TECHNISCHE PRÜFUNG AUF SCHWACHSTELLEN
- SOCIAL-ENGINEERING-TESTS ZUR SENSIBILISIERUNG DER MITARBEITENDEN
- UMSETZUNG VON VERBESSERUNGSMASSNAHMEN

Ansprechpartner

DR. MICHAEL RIECKER
Associate Director
+49 173 575 40 29
michael.riecker@protiviti.de

KAI-UWE RUHSE
Managing Director
+49 172 698 30 39
kai-uwe.ruhse@protiviti.de

KONTAKTIEREN SIE UNS!
+49 69 963 768 100
contact@protiviti.de
www.protiviti.de