IKARUS security software

Ransomware-Attacken: Do‘s and Don’ts

Wer sich plötzlich vor gesperrten Geräten und verschlüsselten Daten wiederfindet, sollte sich bewusst machen: Die Angreifer sind mit hoher Wahrscheinlichkeit nicht eben erst in Ihr Netzwerk eingedrungen, um ihre Ransomware zu platzieren. Rechnen Sie damit, dass sie sich bereits länger in Ihren Systemen umgesehen und zuvor möglicherweise jede Menge sensible Daten mitgenommen haben.

Ein sauberes, funktionierendes Backup ist das Um und Auf, aber es gibt mehr zu beachten.

„Your files are encrypted“ – Jetzt richtig reagieren

Anfang Die richtige Einschätzung der Lage ist im Fall von Cybersecurity Incidents entscheidend – sie ist Voraussetzung dafür, die richtigen Maßnahmen zu ergreifen. Je besser und schneller Sie Ihre Optionen erfassen, umso gezielter und professioneller können Sie reagieren und umso besser stehen Ihre Chancen, Schäden zu minimieren – gleich ob überhöhte Zahlungen, weitere Datenverluste, Rufschädigung, Datenschutzverletzungen oder Produktionsstillstände.

- **Abgeben:** Erwarten Sie nicht, dass die Behörden sofort aktiv auf Ihren Fall eingehen oder Sie gar mit einem Team vor Ort unterstützen können.
- **Eile:** Antworten Sie erstmal NICHT auf die Ransom-Note der Erpresser, andernfalls beginnt die Uhr zu ticken. Strategie ist wichtiger als Tempo.
- **Geheimhalten:** Informieren Sie die Unternehmensleitung darüber, was geschehen ist, welche Maßnahmen bereits gesetzt wurden und welche externen Hilfeleistungen Sie benötigen. Machen Sie unmissverständlich klar, in welchem Umfang Ihre Strukturen betroffen sind und welche Optionen offen stehen.
- **Entscheidungen treffen:** Auch bei Inanspruchnahme externer Hilfe müssen letztendlich Sie – nach kompetenter Beratung – die Entscheidungen für Ihr Unternehmen treffen. Vermeiden Sie unnötige Verzögerungen, diese führen meist nur dazu, dass Ihre Daten publiziert werden.
- **Falsche Erwartungen:** Die Angelegenheit wird sich nicht in wenigen Minuten oder Stunden lösen lassen. Arbeiten Sie gründlich und verhindern Sie damit weitere Risiken. Erwarten Sie nicht, dass Ihr Verhandlungsgeschick die Angreifer umstimmen wird – auch eine Reduktion der geforderten Summe ist nicht „Teil des Spiels“. Vergessen Sie nie, dass der Angreifer ihre finanzielle Situation sehr gut kennt.
- **Emotionen:** Lassen Sie sich nicht von Ihren Emotionen mitreißen. Es ist weder einfach noch angenehm, mit Kriminellen zu verhandeln. Emotionen führen nur zu Reaktionen, die sie bestimmt nicht brauchen können. Setzen Sie daher auf 100%-ige Professionalität.
- **Momentaufnahme:** Erfassen Sie so rasch wie möglich, welche Bereiche in welchem Umfang betroffen sind. Je profunder Ihre Lageeinschätzung ist, umso klarer und schneller können Sie Ihre Optionen ermitteln.
- **Analyse:** Verschaffen Sie sich Klarheit, auch über die Art des Trojaners oder Ransom-as-a-Services. Die meisten Angreifergruppen liefern klare, strukturierte Anweisungen und Hinweise.
- **Teamwork:** Stellen Sie ein kompetentes Team aus internen und externen Expert*innen zusammen, das gemeinsam berät, entscheidet und handelt.
- **Kommunikation:** Informieren Sie Partnerunternehmen und Kund*innen. Eine offene Kommunikationsstrategie kann Ihre Stakeholder davor schützen, über Ihre Infrastruktur angegriffen zu werden oder Datenverluste zu erleiden. Beachten Sie auch die erforderlichen Data-Breach Notification-Maßnahmen.
- **Verhandlungspartner:** Spätestens wenn die Erpresser Kontakt herstellen, sollten Sie einen professionellen Verhandlungsführer an Ihrer Seite haben.

- **Sicherheit:** Setzen Sie sichere Kommunikationswege und ggf. finanzielle Transaktionsmöglichkeiten auf – bereiten Sie alles vor, um Sicherheit und Integrität zu gewährleisten.
- **Strafverfolgung:** Erstatten Sie Anzeige und kontaktieren Sie die Cybercrime-Meldestelle im Bundeskriminalamt unter +43 1 24836 986500 oder against-cybercrime@bmi.gv.at.
- **Notfallplan:** Folgen Sie Ihrem Notfallplan für Ransomware-Angriffe – oder schreiben Sie ihn spätestens jetzt.

Jetzt auf mögliche Angriffe vorbereiten

Mit 304 Millionen Ransomware-Attacken im Jahr 2020 – 62% mehr als noch im Vorjahr – und dem Geschäftsmodell Ransomware-as-Service ist die Frage nicht, ob sondern wann man einem entsprechenden Angriff zum Opfer fällt. Die Unternehmensgröße ist kein Maßstab für Wahrscheinlichkeiten: Mehrere einfachere Ziele sind oft lukrativer als ein großes, schwer zu erreichendes. Die Faustregel lautet daher: Je niedriger die Schutzbarrieren, desto größer ist die Gefahr.

Tipps

Diversifizieren Sie Ihre Backup/Storage Strategien. Sorgen Sie dafür, dass Backups auch extern gelagert werden und verfügbar sind. Verstärken Sie jetzt Ihre Schutzmaßnahmen gegen E-Mail-basierte Angriffe, evaluieren Sie Ihre Endpoint-Lösungen und kontrollieren Sie Remote-Access-Tools. Optimieren Sie Ihre Netzwerksegmentierung und investieren Sie in Maßnahmen zur Früherkennung von Anomalien und Systemschwachstellen.

Lösegeld bezahlen oder nicht?

Die Frage, ob Sie das geforderte Lösegeld bezahlen sollen oder nicht, scheint im ersten Moment die wichtigste – sie ist jedoch bei Weitem nicht die einzige. Wieder zählt eine durchdachte Strategie.

Die Uhr tickt – starten Sie Ihre Maßnahmen in folgender Reihenfolge:

- Incident Response, um bestehende und weitere Fremdzugriffe zu unterbinden
- Investigation, um den Grund für und das Ausmaß des Schadens zu erheben
- Recovery Plan zur Festsetzung der Mittel und Wege zurück zur Geschäftsfähigkeit
- Teambuilding mit internen und externen Spezialisten
- Kommunikation mit Ihren Stakeholdern
- Auseinandersetzung mit den Angreifenden

Behalten Sie bei Ihren Entscheidungen folgende Ziele im Hinterkopf:

- Geschäftsfähigkeit, so weit und sicher als möglich
- Kontrolle über Ihre Systeme
- Erwartungen und Ziele regelmäßig kommunizieren
- Ransomware-Notfallplan mit Ihren Learnings aktualisieren

Berücksichtigen Sie bei Ihren Überlegungen:

- Gefahr durch kompromittierte Daten
- Status und Zustand Ihrer Back-ups
- Aufwand für Neuaufsetzen der gesperrten Geräte
- Zeit und Kosten bis zur Wiederaufnahme der Geschäftstätigkeit
- Zahlungsfähigkeit
- Kosten für Öffentlichkeitsarbeit
- Kosten als Folge des Datenverlusts

Über IKARUS Security Software

Der österreichische Cyber Security Spezialist **IKARUS Security Software GmbH** entwickelt und betreibt seit 1986 führende Sicherheitstechnologien – von der eigenen Scan Engine über Cloud-Services zum Schutz von Endpoints, Mobilgeräten und E-Mail-Gateways bis hin zur modularen Threat Intelligence Plattform.

Mit den Technologie-Partnern Mandiant/FireEye und Nozomi Networks erweitert IKARUS das eigene Portfolio um international marktführende Technologien und ist der österreichische Ansprechpartner für Incident Response und globale wie lokale Threat Intelligence bei IT-/OT-/IoT-Security.

Notfallplan für Sicherheitsvorfälle in IT-, OT- und IoT-Umgebungen:
www.ikarussecurity.com/it-ot-iot-security/ikarus-24-7-incident-response