Leitfaden zur Bewältigung von IT-Sicherheitsvorfällen

Incident Response: Schnell und richtig reagieren

Schnelle und richtige Reaktion auf IT-Sicherheitsvorfälle

IT-Sicherheitsvorfälle können jedes Unternehmen und jede Organisation treffen. Ein gut durchdachter Incident Response Plan hilft, die Auswirkungen von IT-Sicherheitsvorfällen wirksam zu minimieren.

Besonders für Kleinstunternehmen ist ein effizienter Notfallplan wichtig, um auch mit begrenzten Ressourcen effektiv und ohne Verzögerungen oder Unsicherheiten auf Vorfälle reagieren zu können. Dadurch werden Betriebsunterbrechungen minimiert, sensible Daten geschützt, die Sicherheitskultur gestärkt und rechtliche Anforderungen erfüllt.

Bei der Reaktion auf Sicherheitsvorfälle kommt es vor allem auf Schnelligkeit an. Gezielte Gegenmaßnahmen können die technischen und finanziellen Auswirkungen von Cyber-Angriffen erheblich reduzieren und die Wiederherstellung normaler Betriebsabläufe beschleunigen. Daher ist die Implementierung eines effektiven Incident Response Plans für jede Organisation wesentlich, unabhängig von ihrer Größe oder Branche.

Definition von IT-Sicherheitsvorfällen

Klare Vorgaben und Beispiele erleichtern es Anwender*innen, sicherheitsrelevante Vorfälle zu erkennen. Dazu zählen u.a. die folgenden Beispiele:

- **CEO-Fraud-Angriffe:** Versuche, durch gefälschte E-Mails oder Websites an vertrauliche Informationen zu gelangen oder Banktransaktionen zu erzwingen, enden in der Regel mit enormen finanziellen Verlusten. Sensibilisierung schafft Klarheit über solche Phishing-Kampagnen.

- **Ransomware-Infektion:** Schadsoftware, die Dateien oder den gesamten Computer verschlüsselt und Lösegeld für die Wiederherstellung verlangt, müssen sofort gemeldet werden, um eine eventuelle Ausbreitung im System stoppen zu können und ggf. Datendiebstahl zu dokumentieren.

- **Verlust oder Diebstahl von Geräten:** Physische Verluste von Computern, Laptops oder mobilen Geräten mit Zugriff auf Unternehmensressourcen müssen der IT sofort gemeldet werden, um ggf. Geräte oder Benutzer-Konten zu sperren oder Daten via Fernzugriff löschen zu können.

- **Unberechtigter Zugriff auf Systeme:** Der Verdacht auf fremde Zugriffe auf Systeme oder Netzwerke, z.B. auch durch ungewöhnliche Logins, muss der IT sofort gemeldet werden, um Eindringlinge im System erkennen und Sicherheitslücken schließen zu können.

Blechturmgasse 11 | 1050 Wien | Österreich | Tel.: +43 1 589 95-0 | office@ikarus.at | www.IKARUSsecurity.com

Die User-Perspektive: Cyber-Sicherheitsvorfall melden

Die Vorfallmeldung ist der initiale Schritt eines Incident Response-Verfahrens. Schulen und ermutigen Sie Ihre Mitarbeitenden daher laufend, Anzeichen von Sicherheitsverletzungen und Anomalien zu erkennen und umgehend zu melden.

Das angemessene Verhalten bei einem IT-Sicherheitsvorfall ist entscheidend, um die Auswirkungen zu minimieren. Klare Kommunikation von Verhaltensregeln, effizienten Kommunikationswegen, relevanten Ansprechpartnern sowie den essenziellen Informationen, die die IT oder Sicherheitsverantwortlichen zur Vorfallbearbeitung benötigen, fördert eine effektive Zusammenarbeit.

- → Schaffen Sie Bewusstheit für die Gefahren und möglichen Einfallstore.
- → Informieren Sie über aktuelle Bedrohungen wie Ransomware- und Phishing-Kampagnen.
- → Verbreiten Sie Wissen zu beliebten Angriffswegen und geeigneten Gegenmaßnahmen.
- → Positionieren Sie Ihre IT-Abteilung als erster Ansprechpartner für alle Fragen und Vorkommnisse.

Verhaltenstipps für Anwender*innen

- ✓ Bewahren Sie Ruhe!
- ✓ Melden Sie sich telefonisch bei Ihrer IT-Hotline.
- ✓ Stellen Sie sofort Ihre Arbeit mit dem IT-System ein.
- ✓ Dokumentieren Sie, was Sie sehen.
- ✓ Versuchen Sie nicht, das Problem selbst zu lösen!
- ✓ Schalten Sie keinesfalls das System aus („Stecker ziehen“), um keine Spuren zu vernichten.
- ✓ Folgen Sie den Anweisungen Ihrer IT-Abteilung.

Bereiten Sie sich auf folgende Fragen vor:

- → Wer meldet den Vorfall?
- → Welches IT-System ist betroffen?
- → Was haben Sie mit dem IT-System gearbeitet?
- → Was haben Sie beobachtet?
- → Wann ist das Ereignis eingetreten?
- → Wo befindet sich das betroffene IT-System?

Die Zeit ist der wichtigste Faktor bei einem Sicherheitsvorfall. Zögern Sie nicht, sich an die IT zu wenden - lieber ein Anruf zu viel und zu schnell als einer zu wenig!

Blechturmgasse 11 | 1050 Wien | Österreich | Tel.: +43 1 589 95-0 | office@ikarus.at | www.IKARUSsecurity.com

Tipp: Analog zu den bekannten Hinweisschildern „Verhalten im Brandfall“ empfiehlt es sich, alle Büros mit einer sogenannten „**IT-Notfallkarte**“ auszustatten. Diese enthält die richtige(n) Ansprechperson(en) für IT-Notfälle sowie deren Erreichbarkeit, welche Informationen weitergegeben werden sollen sowie Hinweise zu den richtigen Verhaltensweisen.

Die IT-Perspektive: Cyber-Sicherheitsvorfall bearbeiten

Das IT-Personal spielt eine Schlüsselrolle bei der Bewältigung von Sicherheitsvorfällen. Der Grundsatz "Ruhe bewahren" ist auch hier entscheidend, um überlegt zu handeln und die Ausbreitung von Schäden zu minimieren.

Organisatorische und technische Maßnahmen sind gleichermaßen wichtig.

Organisatorische Maßnahmen bei IT-Notfällen

Aus organisatorischer Sicht ist es wichtig zu wissen, welche Stellen wann zu informieren sind.

- ✓ Informieren Sie umgehend IT-Sicherheitsverantwortliche, Datenschutzbeauftragte und den IT-Betrieb.
- ✓ Folgen Sie den vereinbarten Zuständigkeiten für Kommunikation, Eskalation und Meldepflichten.
- ✓ Halten Sie alle Informationen aus der Meldung des IT Security Incidents griffbereit:
    - betroffene Systeme
    - betroffene Benutzer
    - gefundene Anomalien
    - Eintrittsort
    - Verbreitungsweg

Vorhandene Notfallpläne (Incident Response Plans) sollten regelmäßig geübt oder spätestens jetzt erarbeitet werden. Kontaktlisten mit den wichtigsten Ansprechpersonen, Kontaktdaten und Verantwortlichkeiten sollten immer aktuell und griffbereit sein.

Tipp: Etablieren Sie einen alternativen Kommunikationskanal fernab der eigenen IT-Infrastruktur. Die bestehenden Kommunikationskanäle werden unter Umständen bereits vom Angreifer mitgehört.

Technische Maßnahmen bei IT-Notfällen

Beim Umgang mit Rechnern, die von einem Sicherheitsvorfall betroffen sind, ist besondere Vorsicht geboten. Einige allgemeingültige Überlegungen sind zu berücksichtigen.

- → Welche Benutzer-Accounts gibt es auf dem System?
- → Existieren Benutzer-Accounts mit unnötigen, erweiterten Rechten?
- → Wenn ja, wurde diese Änderung am Benutzer erst kürzlich vorgenommen?

Blechturmgasse 11 | 1050 Wien | Österreich | Tel.: +43 1 589 95-0 | office@ikarus.at | www.IKARUSsecurity.com

- → Wer hat die Änderungen am Benutzer durchgeführt? Wann ist dies geschehen?
- → Analysieren Sie nicht nur das betroffene System – halten Sie Ausschau nach weiteren Rechnern, die betroffen sein könnten.
- → Trennen Sie das betroffene System vom produktiven Netzwerk – entweder durch EDR-Lösungen, die dies unterstützen, oder durch Ziehen des Netzwerkkabels, aber keinesfalls durch Ausschalten!
- → Sind mehrere Systeme betroffen, trennen Sie diese möglichst gleichzeitig vom Netzwerk.
- → Sichern Sie forensische Daten (Speicherabbild, Prozesse).
- → Betrachten Sie Systeme als vollständig kompromittiert.
- → Ist ein Benutzerkonto betroffen, betrachten Sie auch das Netzwerk als kompromittiert.
- → Betrachten Sie alle auf betroffenen Systemen gespeicherten bzw. nach der Infektion eingegebenen Zugangsdaten ebenfalls als kompromittiert.
- → Achten Sie auf Vollständig- und Funktionsfähigkeit von Logfiles, insbesondere von Firewall-Logs.
- → Protokollieren Sie den Netzwerkverkehr mit geeigneten Systemen. Sind solche nicht im Einsatz, richten Sie einen Rechner ein, der analysierbaren Netzwerkverkehr über SPAN-Ports bekommt.
- → Blockieren Sie maliziöse Zugriffe auf geeigneten Systemen (z. B. Firewall).
- → Prüfen Sie, ob aktuelle Backups vorhanden sind – und ob diese kompromittiert sein könnten!

Achtung: Niemals darf sich ein Administrator-Account auf einem kompromittierten System anmelden! Dies darf - sofern notwendig - nur erfolgen, wenn das System vom Netzwerk getrennt ist!

Protokolldaten untersuchen

Als nächstes werden die Logdaten untersucht, wobei die Protokolle der Firewall, des Proxys, des Mailservers und des Active Directory von besonderem Interesse sind. Unerlaubte Zugriffsversuche, IP-Adressen von Angreifern, verdächtige URLs oder Downloads, Phishing- oder Spam-Mails, fehlgeschlagene oder verdächtige Authentifizierungs- oder Anmeldeversuche, Änderungen an Benutzerkonten oder ungewöhnliche Zugriffsaktivitäten können so identifiziert werden.

Die Interpretation dieser Daten erfordert erfahrenes Personal, das mit den normalen Vorgängen vertraut ist, um bösartige Veränderungen nach der Infektion zu erkennen.

System neu aufsetzen und sichern

Das betroffene System sollte neu aufgesetzt werden, um sicherzustellen, dass keinerlei Rückstände oder Spuren der Schadsoftware verbleiben. Im Anschluss daran ist es wichtig, aus dem Vorfall zu lernen: Wie konnte die Schadsoftware das System infiltrieren? Die neu aufgesetzten Systeme müssen gehärtet, der Eintrittsvektor geschlossen werden.

Blechturmgasse 11 | 1050 Wien | Österreich | Tel.: +43 1 589 95-0 | office@ikarus.at | www.IKARUSsecurity.com

Beim Wiederanlauf der IT-Systeme sollte eine bestimmte Reihenfolge eingehalten werden, wobei kritische Systeme zuerst wieder hochgefahren bzw. in Betrieb genommen werden. Checklisten helfen bei der Umsetzung.

Ressourcen:

- → IKARUS Incident Response Checkliste für KMU
- → IKARUS Notfallplan bei Ransomware
- → IT-Notfallkarte "Verhalten bei IT-Notfällen" (BSI)
- → Meldung von Datenschutzverletzungen (WKO)

Services:

- → IKARUS 24/7 incident.response: Notfallservice für Cyber-Sicherheitsvorfälle
- → SECUTAIN Awareness-Kampagnen, Awareness Pakete, Beratung & Schulung

Über IKARUS Security Software GmbH

Seit 1986 ist IKARUS Security Software an vorderster Front der Entwicklung und Implementierung von Cyber-Security-Lösungen. Die eigene Malware Scan Engine, benutzerfreundliche Cloud-Lösungen und die Absicherung kritischer Infrastrukturen stehen dabei im Fokus.

In Zusammenarbeit mit globalen Marktführern bietet IKARUS umfassende Cybersecurity-Services für Organisationen jeder Größe sowie für kritische Infrastrukturen an – von Incident Response Services über Advanced Threat Protection und OT-Security-Sensoren bis hin zur modularen IKARUS Threat Intelligence Platform. Die Integration von Partner-Technologien in das IKARUS Rechenzentrum in Wien gewährleistet dabei volle Transparenz und Sicherheit bei der Datenverarbeitung.

Blechturmgasse 11 | 1050 Wien | Österreich | Tel.: +43 1 589 95-0 | office@ikarus.at | www.IKARUSsecurity.com