Richtige Reaktion auf IT-Sicherheitsvorfälle

Verhalten bei einem Security Incident – die User Perspektive

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) liefert für den deutschsprachigen Raum stets aktualisierte Standards und Regelwerke, an denen sich Unternehmen unterschiedlichster Größe orientieren können. Dazu gehören auch empfohlene Verhaltensweisen für Cyber-Sicherheitsvorfälle. Die wichtigsten Punkte daraus sind:

- 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“, „Akku entfernen“) – dies könnte wichtige digitale Spuren verwischen!
- Ihre IT-Hotline wird Sie über zu ergreifende Maßnahmen informieren.

Die IT-Hotline wird Ihnen folgende Fragen stellen:

- 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?

Beachten Sie, dass Zeit bei einem Sicherheitsvorfall die wichtigste Komponente ist – zögern Sie also nicht, sich an die IT zu wenden! Besser, ein Anruf zu viel und zu schnell, als einer zu wenig!

Verhalten bei einem Security Incident – die IT Perspektive

Dem IT-Personal kommt bei einem Sicherheitsvorfall besondere Verantwortung zu. Dabei gilt es sowohl organisatorische als auch technische Themen zu bedenken. Die wichtigsten Grundsätze sind jedoch auch hier:

- Bewahren Sie Ruhe!
- Handeln Sie auch unter Stress stets überlegt!

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

IT Perspektive: Organisatorische Tätigkeiten bei IT-Notfällen

Je nach Unternehmensgröße kann es unterschiedliche Vorarbeiten geben, die für einen IT-Notfall bereits getroffen wurden oder, wenn Sie damit gerade am Beginn stehen, zu treffen sind. Organisatorisches Um und Auf ist zu wissen, welche Stellen informiert werden müssen und wann dies zu geschehen hat.

- Informieren Sie den IT-Sicherheitsverantwortlichen, Datenschutzbeauftragte und den IT-Betrieb
- Diese Stellen kümmern sich üblicherweise um die weitere Koordination, Behandlung von Meldepflichten…
- Halten Sie griffbereit, was passiert und wie dies aufgefallen ist – siehe Informationen aus der User Perspektive

In größeren Unternehmen gibt es in der Regel ausgearbeitete Notfallpläne (Incident Response Pläne), die sich je nach betroffenem IT-System unterscheiden können. Diese sollten immer wieder geprobt werden. Auch für kleine Unternehmen ist es hilfreich, eine kurze Checkliste mit den wichtigsten Kontakten und Tätigkeiten anzulegen, an der man sich im Ernstfall orientieren kann.

IT Perspektive: Technische Tätigkeiten bei IT-Notfällen

Beim Hantieren mit Rechnern, die von einem Sicherheitsvorfall betroffen sind, ist besondere Vorsicht geboten. Einige allgemeingültige Grundsätze sind zu berücksichtigen. Dazu zählen die folgenden Punkte:

- Welche Benutzerkonten existieren auf dem System?
- Haben diese unnötige erweiterte Rechte?
- Wenn ja, wurde diese Änderung am Benutzer erst kürzlich vorgenommen?
- 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, 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.
- Achten Sie auf Vollständig- und Funktionsfähigkeit von Logfiles, insbesondere von Firewall-Logs.
- Protokollieren Sie Netzwerkverkehr mit dafür geeigneten Systemen. Wenn Sie solche nicht im Einsatz haben, richten Sie einen Rechner ein, der analysierbaren Netzwerkverkehr über SPAN Ports bekommt.
- Wenn alle verantwortlichen Personen maliziöse Zugriffe gefunden haben, blockieren Sie diese auf geeigneten Systemen (z. B. Firewall).
- Prüfen Sie, ob aktuelle Backups vorhanden sind – und ebenso, ob diese kompromittiert sein könnten.

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

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

Der erste Schritt ist die Erstellung eines forensischen Systemabbilds inkl. der Speicher- und Prozessinformationen. Ein forensisches Festplattenimage ist eine exakte Sektorkopie der Festplatte des betroffenen Systems. Bei virtuellen Systemen ist es ausreichend, das Verzeichnis der Virtualisierungssoftware zu sichern; beim „suspend“ einer virtuellen Maschine wird ein Dump des Arbeitsspeichers abgelegt und kann zum Auswerten der Daten herangezogen werden. Die Incident Response arbeitet dann nur noch mit der Kopie der Daten, nicht mit dem schadhaften System selbst.

Danach werden Logdaten gesichtet, dabei sind insbesondere Firewall, Proxy, Mailserver und Active Directory Logs von Interesse. Für die Interpretation dieser Files braucht man versiertes Netzwerkpersonal, das gut über normale Vorgänge Bescheid weiß, um die maliziösen Änderungen, die nach der Infektion passiert sind, erkennen zu können.

Das betroffene System sollte neu aufgesetzt werden, damit sicher keine Spuren zurückbleiben. Dann geht es darum, aus dem Vorfall zu lernen: Wie kam die Schadsoftware auf das System? Die neu aufgesetzten Systeme müssen gehärtet, der Eintrittsvektor geschlossen werden. In einem Incident Fall sollte auf Remote Access wie etwa Teamviewer, RDP o.ä. verzichtet und ausschließlich lokal gearbeitet werden. Beachten Sie beim Wiederanlauf der IT-Systeme eine bestimmte Reihenfolge, kritische Systeme müssen zuerst wieder hochgefahren bzw. ans Netz gebracht werden. Dabei helfen Checklisten.

IKARUS 24/7 incident.response: Notfallplan für Sicherheitsvorfälle in IT, OT oder IoT Umgebungen

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.