Verhaltensregeln

10 Schritte im IT-Sicherheitsnotfall

Gehen Sie koordiniert und Schritt für Schritt vor. Betrachten Sie die ggf. betroffenen IT-Systeme als einen Tatort. Unkoordinierte Handlungen führen schnell dazu, dass Spuren verändert und hierdurch wichtige Beweismittel vernichtet werden. Bedenken Sie: Bei einem Mord würden Sie das Mordwerkzeug auch nicht anfassen. Lassen Sie das System daher unverändert.

1. Verändern Sie das System nicht

Schalten Sie z.B. das System auf keinen Fall aus und führen Sie keinen Neustart des Rechners oder dergleichen durch. Flüchtige Spuren (z.B. im Arbeitsspeicher) könnten hierdurch vernichtet werden.

2. Sichern Sie mögliche Beweismittel

Schränken Sie den Zugang zu möglichen Beweismitteln (z.B. Desktoprechner, Smartphones, USB-Sticks etc.) ein, bis diese forensisch gesichert wurden.

3. Protokollieren Sie Ihre Schritte

Protokollieren Sie durchgängig jeden einzelnen Schritt! Dokumentieren Sie beispielsweise unbedingt wer wann wo Zugriffsmöglichkeiten auf die Beweismittel hatte. Fotografieren Sie die lokalen Gegebenheiten.

4. Informieren Sie die relevanten internen Stellen

Informieren Sie das Management, die Rechtsabteilung, den IT-Sicherheitsbeauftragten sowie den betrieblichen Datenschutzbeauftragten über den Sicherheitsvorfall. Legen Sie anschließend gemeinsam fest, welche weiteren internen Stellen ggf. informiert werden müssen (z.B. Personalabteilung, Compliance- oder Revisionsabteilung, Presseabteilung oder Betriebsrat). Denken Sie aber daran, der Täter wurde noch nicht gefasst. Soweit daher auch interne Stellen zum potentiellen Täterkreis gehören, weiten Sie den Kreis der informierten Personen nicht unnötig aus.

5. Benennen Sie eine verantwortliche Leitungsperson

Benennen Sie eine Person, welche die Aufklärung und Bearbeitung des Sicherheitsvorfalls intern koordiniert und beispielsweise Schnittstellen zu externen Dienstleistern (u.a. IT-Forensiker) bildet.

6. Ermitteln Sie den Sachverhalt

Ermitteln Sie, was genau (Art, Umfang, Datum) passiert ist bzw. zu sein scheint. Handelt es sich z.B. um einen Abfluss von Betriebs- oder Geschäftsgeheimnissen, wer kommt als Täter in Frage, wie und wann ist dies konkret vorgefallen, welche Umstände lassen auf eine fahrlässige oder vorsätzliche Begehung schließen und welche Systeme sind relevant? Oder handelt es sich um eine Hackerattacke? Welche Systeme sind in diesem Fall potentiell davon betroffen und welche Anhaltspunkte gibt es hierfür?

7. Schalten Sie IT-Forensik-Experten ein

Sofern Sie keine IT-Forensiker beschäftigen, holen Sie sich externe Hilfe, um den Sachverhalt so aufzuklären und aufzuarbeiten, dass dieser auch die Voraussetzungen für ein potentielles späteres Gerichtsverfahren erfüllt. IT-Forensiker sind darauf spezialisiert, vorhandene digitale Spuren gerichtsfest forensisch zu sichern, zu analysieren und anschließend zu präsentieren.

8. Informieren Sie externe Stellen

Klären Sie mit der Unternehmensführung, der Rechtsabteilung und dem betrieblichen Datenschutzbeauftragten ab, ob ggf. externe Stellen (u.a. Aufsichtsbehörden oder von einem Datendiebstahl betroffene Personengruppen) über den Sicherheitsvorfall informiert werden müssen. Einige Gesetze (z.B. DSGVO, TMG oder IT-Sicherheitsgesetz) verlangen u.U. entsprechende Informationsweitergaben und es drohen bei Nicht-Einhaltung Bußgelder.

9. Beseitigung

Beseitigen Sie schließlich die von den IT-Forensik-Experten identifizierten Bedrohungen. Blocken Sie beispielsweise bösartige IP-Adressen, ändern Sie die unternehmensweiten Passwörter und verifizieren Sie die Neugestaltung. WICHTIG: Stellen Sie unbedingt sicher, dass zuvor alle kompromittierten Systeme identifiziert wurden! Ansonsten warnen Sie ggf. die Angreifer, was dazu führt, dass weitere Hintertüren in Ihre Systeme implementiert oder Daten exfiltriert oder beschädigt werden.

10. Wiederherstellung und Lessons Learned

Nachdem Sie die akute Bedrohung beseitigt haben, verbessern oder implementieren Sie anschließend Lösungen zum Langzeitschutz. Redesignen Sie beispielsweise Ihr Netzwerk (Stichwort Netzsegmentierung), zentralisieren Sie das Logging (SIEM) oder optimieren Sie Ihr Security Awareness Training. Nutzen Sie den Sicherheitsvorfall sodann als Lerneffekt für die Zukunft. Halten Sie beispielsweise nach neuen Bedrohungen Ausschau und führen Sie regelmäßige Pentests sowie IT-Sicherheitsaudits durch.

Joanna Lang-Recht
Head of IT Forensics

24/7 IT-Notfallhilfe

0180 622 124 6

20 Ct./Anruf aus dem Festnetz, Mobilfunk max. 60 Ct./Anruf

Direkt Kontakt aufnehmen

› it-forensik@intersoft-consulting.de

Weitere Infos auf unserer Webseite

› www.it-forensik.de