consol

ICH HABE EINEN IT-SICHERHEITS-VORFALL – WAS NUN?

CONSOL CHECKLISTE

In der Informationssicherheit spricht man von Informationssicherheitsereignissen und Informationssicherheitsvorfällen. Was verstehen wir darunter?

Bei einem Informationssicherheitsereignis wurde ein Ereignis bei einem System, Service oder Netzwerk ermittelt, das auf eine mögliche Verletzung der Richtlinien zur Informationssicherheit oder auf ein Fehlschlagen einer Sicherheitsmaßnahme hindeutet.

Bei einem Informationssicherheitsvorfall sind ein oder mehrere unerwartete Informationssicherheitsereignisse aufgetreten, die wahrscheinlich den Geschäftsbetrieb und die Informationssicherheit gefährden.

Anhand der beiden folgenden Checklisten möchten wir Ihnen einen allgemeinen Leitfaden an die Hand geben, der Sie dabei unterstützen soll, sich auf einen IT-Notfall vorzubereiten und diesen strukturiert zu bewältigen.

Checkliste „Organisatorisches“

1. Bewahren Sie Ruhe. Wissen alle, die intern davon wissen müssen, von dem IT-Notfall?
   - Sind der IT-Betrieb, der IT-Sicherheitsverantwortliche und der Datenschutzbeauftragte informiert?
   - Ist die Geschäftsleitung informiert?
   - Sind alle internen Stellen informiert?

2. Organisieren Sie sich. Verteilen Sie Rollen und Zuständigkeiten.
   - Wer trifft die relevanten Entscheidungen?
   - Wer erledigt was bis wann?

3. **Sammeln Sie Informationen zum IT-Sicherheitsvorfall, um darauf aufbauend Entscheidungen treffen zu können.**
   - Was ist genau passiert?
   - Wie ist es aufgefallen?
   - Welche Auswirkungen kann der Vorfall direkt auf das Unternehmen und seine Kerndienstleistungen haben?
     Muss der Weiterbetrieb gewährleistet werden?
     Besteht genügend zeitlicher Spielraum, um das Problem umfassend analysieren und bewältigen zu können?

Ist eine Strafverfolgung vorgesehen? Muss deshalb beweissicher gehandelt werden?
- Welche Auswirkungen hat der IT-Sicherheitsvorfall auf Kunden/Partner/Öffentlichkeit?
- Warum ist der IT-Sicherheitsvorfall bei uns passiert? Gibt es Hinweise auf ein gezieltes, gegen uns gerichtetes Vorgehen oder sind wir nur eines von vielen potentiellen Opfern?

4. Berücksichtigen Sie folgende Kommunikationsaspekte

- Schaffen Sie die Rolle eines zuständigen Kommunikationsexperten, der Informationen abgestimmt, gezielt und gebündelt verteilen, aber auch entgegennehmen kann.
- Vernachlässigen Sie nicht die Benachrichtigung Ihrer Mitarbeitenden.
- Prüfen Sie, wer informiert werden muss oder sollte.
- Gibt es bestehende Meldepflichten? Im Falle einer Datenschutzverletzung ist der IT-Vorfall an die zuständige Datenschutzaufsichtsbehörde zu melden.
- Gelten vertragliche Informationspflichten gegenüber Auftraggebern, Geschäftspartnern, Auftragnehmern oder Versicherungen?
- Muss die Öffentlichkeit miteinbezogen werden?
- Möchten Sie den IT-Sicherheitsvorfall freiwillig melden, um die Warnung potentiell weiterer Betroffener zu ermöglichen?
- Wollen Sie Strafanzeige stellen?

5. Falls Bedarf besteht, suchen Sie sich externe Unterstützung.

- Ansprechpartner finden Sie über die zuständige Industrie- und Handelskammer oder das Bundesamt für Sicherheit in der Informationstechnik (BSI).

6. Nachbereitung

- Lernen Sie aus dem IT-Sicherheitsvorfall.
- Bereiten Sie sich jetzt schon auf den nächsten Angriff vor.

Checkliste „Technik“

1. Keine Anmeldung mit privilegierten Nutzerkonten auf einem potentiell infizierten System

- Gibt es Benutzerkonten mit unnötigen, privilegierten Rechten?
- Gibt es Hinweise darauf, dass die privilegierten Rechte durch Unbefugte erst in jüngster Vergangenheit eingerichtet wurden?

2. Stellen Sie sicher, dass Sie vollständige und aktuelle Informationen über Ihr Netzwerk verwenden.

- Identifizieren Sie das betroffene System oder die betroffenen Systeme.
- Trennen Sie die betroffenen Systeme vom internen produktiven Netzwerk und dem Internet:
    - Ziehen Sie das Netzwerkkabel.
    - Fahren Sie das Gerät nicht herunter oder schalten Sie es aus, sofern eine technische Analyse beabsichtigt ist.
    - Erstellen Sie gegebenenfalls eine forensische Sicherung inkl. Speicherabbild, sofern eine Strafverfolgung eingeleitet werden soll.
    - Setzen Sie im Anschluss ein Antiviren-Programm ein.

- Betrachten Sie infizierte lokale Systeme grundsätzlich als vollständig kompromittiert. Planen Sie eine komplette Neuinstallation ein.
- Betrachten Sie alle auf betroffenen Systemen gespeicherten eingegebenen Zugangsdaten als ebenfalls kompromittiert.
- Sollte das Active Directory (AD) kompromittiert sein, betrachten Sie das gesamte Netz als kompromittiert.

3. Richten Sie in Abstimmung mit Ihrem Datenschutzbeauftragten ein ausreichendes Netzwerk-Monitoring und Logging ein.

- Als Best Practice gilt das Full-Packet-Capturing im Netzwerk:
    - Am Mirror-Port an internen, zentralen Netzkoppelelementen können die Kommunikation der infizierten, internen Systeme untereinander oder der lokalen Command & Control Server erkannt werden.
    - Am Übergang zwischen LAN und WAN (Wide Area Network) können die externen C&C-Server festgestellt werden.
    - Angriffe werden zumeist durch Externe festgestellt und an Betroffene gemeldet. Um eine solche Meldung nachvollziehen zu können, muss an der Firewall geloggt werden.

- Richten Sie dezidierte Protokollserver ein. Diese sollten außerhalb des Produktiv/-Büronetzes über eine Schnittstelle im „Promiscuous-Mode“ betrieben werden.
- Blockieren Sie jetzt erkennbare Täterzugänge.

4. Prüfen Sie, ob Sie über aktuelle und saubere Backups verfügen.

- Bewahren Sie diese optimalerweise offline auf. Online-Sicherungen könnten bewusst kompromittiert worden sein.

Quellen: Bundesamt für Sicherheit in der Informationstechnik
https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Unternehmen/Ich-habe-einen-IT-Sicherheitsvorfall-Checkliste-Organisatorisches/ich-habe-einen-it-sicherheitsvorfall-checkliste-organisatorisches_node.html

https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Unternehmen/Ich-habe-einen-IT-Sicherheitsvorfall-Checkliste-Technik/ich-habe-einen-it-sicherheitsvorfall-checkliste-technik_node.html

ConSol
Consulting & Solutions Software GmbH

St.-Cajetan-Straße 43
D-81669 München
Tel.: +49-89-45841-100
vertrieb@consol.de
www.consol.de
Folgen Sie uns auf LinkedIn:
@consol-software-gmbh

ConSol
Austria Software GmbH

Maysedergasse 2/25
A-1010 Wien, Österreich
Tel.: +43-1-9971392
info-austria@consol.com
www.consol-software.at
Folgen Sie uns auf LinkedIn:
@consol-austria-software-gmbh