Incident Response Plan

Handlungsempfehlung
bei Cyber-Attacken

Die Qualität und der Umfang an Cyber-Attacken nehmen ständig zu. Unternehmen müssen sich in diesem Zusammenhang im Klaren sein, dass man sich auch mit grossen Investitionen nicht 100% vor diesen Angriffen schützen kann.

Technische Innovationen machen Hackerangriffe immer ausgefeilter und gefährden die Systemverfügbarkeit. Und das wird sich auch zukünftig nicht ändern. Denn in dem Masse, wie sich die technischen Möglichkeiten weiterentwickeln, werden Cyber-Kriminelle daran arbeiten, diese zu ihren Gunsten zu nutzen.

Es ist wichtig, dass Unternehmen für den Fall der Fälle vorgesorgt haben und die **Business Continuity** sicherstellen können. Business Continuity umfasst Massnahmen und Prozesse, um die Folgen einer Betriebsunterbrechung (z.B. nach einer Cyber-Attacke) zu minimieren. Der Themenbereich Business Continuity umfasst Strategien, Pläne, Massnahmen und Prozesse. Im vorliegenden Dokument beschäftigen wir uns mit dem Thema «Pläne».

Mit dem hier vorliegenden «Incident Response Plan» wollen wir Sie auf den Eintritt möglicher Ereignisse (Cyber-Attacken) vorbereiten und Ihnen helfen im Falle eines Angriffs richtig zu reagieren. Im Ernstfall ist es wichtig, dass Sie sofort eine koordinierende Stelle einrichten, welche für ein einheitliches Vorgehen sorgt.

Ihr Vorgehen sollte nach den folgenden Schritten ablaufen

1. **Bei Verdacht oder konkreten Erkenntnissen:** Informieren Sie umgehend ihren IT-Partner oder arcade telefonisch unter +41 41 417 31 70. Geben Sie bitte an, dass es sich um einen «kritischen Security Incident» handelt.

2. **Weiteres Schadensausmass verhindern:** Trennen Sie potenziell infizierte Geräte sofort vom Netzwerk (Netzwerkkabel entfernen und/oder deaktivieren der WLAN-Verbindung). Falls Sie Citrix verwenden, melden Sie sich aus der Session ab (nicht «Session trennen»).

3. **Backupdaten schützen:** Trennen Sie, sofern möglich, Datenträger mit Back-up-Daten ebenfalls umgehend von der Infrastruktur. Sollten Sie sich nicht sicher sein, warten Sie auf konkrete Anweisungen oder Massnahmen seitens ihres IT-Partners bzw. arcade.

4. **Organisation einer internen Taskforce:** Bilden Sie auf Führungsebene eine interne TaskForce, welche sich dem Vorfall annimmt. Die Interaktion zwecks Eingrenzung, Analyse und Behebung des aktuellen Vorfalls findet zwischen diesem Gremium und Ihrem IT-Partner (arcade) statt. Mitarbeiter werden durch den IT-Partner (arcade) nicht direkt kontaktiert.

5. **Reaktion auf Erpressungen oder Kommunikationsversuche seitens Angreifer:** Reagieren Sie keinesfalls übereilt auf irgendwelche Forderungen oder Kommunikationsversuche (E-Mail usw.) seitens der Angreifer. Informieren Sie Ihre Mitarbeiter, dass Sie sich in solchen Fällen an ihre Vorgesetzen wenden sollen.

6. **Verantwortungsübernahme gegenüber Kunden und Partnern:** Versuchen Sie intern zu analysieren, ob und welche Daten betroffen sein könnten. Sollten möglicherweise Kundendaten betroffen sein, führen Sie bitte diese Kunden auf und stellen die entsprechenden Kontaktdaten bereit. Dadurch wird eine zeitnahe und proaktive Information der betroffenen Kunden ermöglicht. Sollten Personendaten betroffen sein – Information des jeweiligen Datenschutzbeauftragen des Kantons oder den Eidgenössischen Datenschutzbeauftragten (EDÖB). Ihr IT-Partner (arcade) wird Sie beraten und Ihnen die notwendigen Kontaktdaten zur Verfügung stellen.

7. **Anzeige erstatten:** Diskutieren Sie, ob eine Strafanzeige gegen die Angreifer für Sie in Betracht kommt. arcade wird Sie bei Ihrer Entscheidung beratend unterstützen und die notwendigen Kontakte zur Verfügung stellen.

8. **Eingrenzung, Analyse und Behebung:** Ihr IT-Partner (arcade) wird Sie bei allen weiteren Schritten unterstützen und die notwendigen Massnahmen mit Ihnen gemeinsam umsetzen.

Weiter zu beachten:

Kein Kontakt mit Angreifern	Wir empfehlen grundsätzlich, keinen Kontakt mit den Angreifern aufzunehmen oder auf Lösegeldforderungen einzugehen. Ansonsten finanzieren Sie direkt die Kriminellen, welche diese Ressourcen in den Ausbau ihrer Infrastruktur investieren um weitere Opfer zu erpressen. Zudem gibt es keine Garantie, dass Sie tatsächlich die Schlüssel für die Wiederherstellung ihrer Daten erhalten. Das weitere Vorgehen sollte zwischen der kundenseitig gebildeten Taskforce und dem IT-Partner (arcade) besprochen werden.
Information leakage	Es besteht das Risiko, dass die Angreifer Unternehmensinformationen entwenden und diese veröffentlichen. Bereiten Sie sich auf solche Szenarien vor und definieren Sie, wer in solchen Fällen für die Kommunikation zuständig ist.
Strafanzeige	Um eine Strafanzeige zu ermöglichen ist es notwendig, alle Vorgänge im Detail zu dokumentieren. Weisen Sie ihre Mitarbeiter daraufhin, nicht eigenmächtig Daten zu löschen und nehmen Sie Kontakt mit ihrem IT-Partner (arcade) auf.
Kommunikation	Es wird empfohlen gegenüber Kunden proaktiv zu kommunizieren. Bei grösseren Ereignissen sollte auch eine Kommunikation über entsprechende Medien in Betracht gezogen werden. Ein Mitglied der Taskforce sollte sich für den Bereich Kommunikation verantwortlich zeichnen.

Ihr IT-Partner (arcade) unterstützt Sie bei allen erforderlichen Schritten und Massnahmen. Bevor Sie Anzeige erstatten oder extern kommunizieren, sollte in jedem Fall Ihr IT-Partner (arcade) für eine entsprechende Analyse und Schadensbegrenzung beigezogen werden. Nun wünschen wir Ihnen alles Gute und hoffen, dass Sie diesen Notfall-Plan nie anwenden müssen. Wenn doch, dann wird unser «Incident Response Plan» Ihnen hoffentlich gute Dienste erweisen.

Sollte sich ein Vorfall ereignen, dann zögern Sie nicht uns zu kontaktieren und um Rat zu fragen.

Kontakt im Notfall

Telefon	+41 41 417 31 70
E-Mail	support@arcade.ch
Stichwort:	**«kritischer Security Incident»**

arcade solutions ag • Winkelriedstrasse 37 • 6003 Luzern • +41 41 417 31 73 • arcade.ch