stoïk

Leitfaden zur Prävention und Unterstützung bei Cybervorfällen

Vorstellung

In diesem Dokument werden zwei wichtige Elemente der Absicherung des Versicherten behandelt:

- **Prävention:** Tools von Stoïk, die Sie sofort einsetzen können, um eine Gefährdung durch Cyberrisiken zu verringern;
- **Unterstützung und Schadensmanagement**: Richtige Reflexe bei einem Cybervorfall und Ablauf des Entschädigungsprozesses.

Am Ende des Dokuments finden Sie außerdem Tipps zur Verbesserung der Cybersicherheit.

Prävention

Im Rahmen seiner Cyber-Versicherungspolice stellt Stoïk dem Versicherten verschiedene Präventionstools zur Verfügung.

Diese Tools überwachen die von Hackern am häufigsten genutzten Zugangspunkte und können so die Häufigkeit der Vorfälle um den Faktor 4 reduzieren.

Präventionstool	Wie schützt es den Versicherten?	Status
Externer Scan	Ein automatisiertes wöchentliches Audit, um zu verhindern, dass Sicherheitslücken ausgenutzt werden, durch die Hacker in das IT-System eindringen können	Installiert
Phishing-Simulation	Gefälschte Phishing-E-Mails und Sensibilisierungsmodule, um Ihre Teams in Cybersicherheit zu schulen	Muss installiert werden (≈ 5 min)
Active Directory Scan (AD)	Eine Prüfung auf zu permissive Benutzerrechte, veraltete Systeme, eine schwache Passwortpolitik	Muss installiert werden (≈ 5 min)
Cloud-Scan (Amazon Web Service, Microsoft Azure)	Eine automatisierte wöchentliche Analyse der Cloud-Konfigurationen (Backups, Rechte, Firewall), um eine Verbreitung des Angreifers im IT-System zu stoppen	Muss installiert werden (≈ 5 min)

Einrichten von Präventionstools

Wählen Sie die gewünschte Methode zum Einrichten der Tools:

- Selbstständig: Der Installationsprozess ist für jedes Tool im Hilfezentrum von Stoïk detailliert beschrieben;
- Mit Betreuung durch einen Stoïk-Experten: Der Versicherte muss sich an seinen Makler wenden, um ein Meeting zur Einführung der Cyber-Tools auszumachen. Alternativ kann der Versicherte direkt einen Termin über folgenden Link vereinbaren.

Unterstützung im Schadensfall

Im Falle eines nachgewiesenen oder vermuteten Cyberangriffs sollte der Versicherte Stoïk sofort unter der Nummer +49 221 95673344 (24-Stunden-Service) kontaktieren. Unsere Schadenmanagement-Experten werden ab dem Moment des Anrufs aktiv.

Es ist von entscheidender Bedeutung, möglichst wenig Änderungen im IT-System selbständig vorzunehmen, damit die für die Untersuchung notwendigen Spuren des Angreifers erhalten bleiben.

Support

Das 24/7 verfügbare Incident Response Team Stoïk-CERT hat eine durchschnittliche Antwortszeit von 3 Minuten. Das Team beginnt sofort mit dem Schutz und der Widerherstellung der Systeme. Gleichzeitig kümmern wir uns um den Kontakt zu den zuständigen Instanzen (Datenschutzbehörde) und beauftragen bei Bedarf Anwälte und Experten für Krisenkommunikation.

Behebung

Stoïk-CERT stellt die Infrastruktur im Durchschnitt in weniger als 12 Stunden wieder her, sodass der Betrieb schnell wieder aufgenommen werden kann. Unsere Experten greifen remote auf das IT-System zu. In Ausnahmefällen kann auch direkt vor Ort eingegriffen werden, wenn es die Situation erfordert.

Entschädigung

Wir benötigen von dem Versicherten eine Liste an Informationen, die wir zur Schätzung des Schadens benötigen. Sobald wir die Informationen erhalten haben, wird die Schadenshöhe geschätzt - dazu kann ein Sachverständiger beauftragt werden. Daraufhin versenden wir ein Schreiben mit der Bestätigung der Deckung und der Höhe: Sobald die Entschädigung zugesagt ist, wird sie ausgezahlt.

Vertragliche Verpflichtungen des Versicherten

- Sobald ein Cyberangriff vermutet wird, sollte Stoïk kontaktiert werden: Je früher unsere Experten eingeschaltet werden, desto geringer ist der Schaden und die Schwere des Angriffs. Bei einem Fehlalarm fallen keine Kosten an;
- Wenn Stoïk mehr als 48 Stunden nach Entdecken des Angriffs kontaktiert wird, riskiert der Kunde den Verlust des Versicherungsschutzes;
- Nach Möglichkeit sollten keine Kosten entstehen, bevor der Versicherungsnehmer sich mit Stoïk in Verbindung gesetzt hat.

Tipps zur Cybersicherheit für Versicherungsnehmer

Zusätzlich zu den Präventionstools werden im Folgenden drei Maßnahmen empfohlen, um eine Kultur der Cybersicherheit innerhalb der Teams des versicherten Unternehmens zu fördern.

---

1. Starke Passwörter erstellen

Warum das wichtig ist: Die Passwörter der Mitarbeiter sind wie ein Einfallstor zum IT-System des Unternehmens.

Was Sie tun sollten: die Mitarbeiter dazu anhalten, Passwörter zu erstellen, die mindestens 14 Zeichen lang und für jede Anwendung unterschiedlich sein sollten; einen Passwortmanager installieren, um automatisch starke Passwörter zu generieren, die an einem sicheren Ort gespeichert werden. Klicken Sie hier, um unser Sensibilisierungsmodul zu diesem Thema anzusehen.

2. Besonders wachsam sein bei Zahlungsaufforderungen

Warum das wichtig ist: Jedes Jahr werden zahlreiche Unternehmen Opfer von Betrugsfällen, bei denen manchmal bis zu mehreren Millionen Euro erbeutet werden.

Was Sie tun sollten: Mitarbeiter, insbesondere die Support-Teams, für die richtigen Verhaltensweisen sensibilisieren, wenn sie eine Aufforderung zu Geldtransfers erhalten. Klicken Sie hier, um unser Sensibilisierungsmodul zu diesem Thema anzusehen.

3. Zwei-Faktor-Authentifizierung (2FA) einrichten

Warum das wichtig ist: Die Zwei-Faktor-Authentifizierung (2FA) erhöht die Sicherheit von Online-Plattformen, indem sie zwei Arten der Verifizierung verlangt - die erste über das Passwort und die zweite über einen Code, der per E-Mail oder SMS versendet wird.

Was Sie tun sollten: Die Mitarbeiter dazu anhalten, 2FA zu aktivieren, sobald dies angeboten wird, um Online-Konten zusätzlich zu schützen.

Maßgeschneiderte Cybersicherheit-Betreuung

Unser Ziel bei Stoïk ist es, Cyberrisiken zu vermeiden und im Schadensfall eine optimale Kundenerfahrung zu bieten. Versicherten Unternehmen, die eine zusätzliche Cybersicherheit-Betreuung durch uns, das Einrichten von Präventionstools oder die Behebung technischer Schwachstellen wünschen, empfehlen wir, sich vorab mit ihrem Makler in Verbindung zu setzen.