schönherr
ATTORNEYS AT LAW

Checklisten zur Vorbereitung auf einen Cyberangriff und für den Cybernotfall

Vorbereitung auf einen Cyberangriff – Checkliste für einen sicheren Sommer

Der wohlverdiente Urlaub steht bevor - doch Cyberangriffe haben gerade in der Urlaubszeit Hochkonjunktur!

Ist Ihr Unternehmen auch während dieser Zeit ausreichend geschützt?

Gute **Vorbereitung** ist essenziell!

Packen wir gemeinsam einige Tipps und Hilfestellungen in Ihr (digitales) Reisegepäck:

- ☐ Sind die **Rollen und Zuständigkeiten** im Notfall **klar** definiert und wurden Urlaubsabwesenheiten im Team abgestimmt?
- ☐ Ist sichergestellt, dass die **Belegschaft** – auch bei Abwesenheit der Geschäftsleitung – auf typische Cyber- und Social-Engineering-Angriffe **sensibilisiert** ist, adäquat darauf reagiert, die **Meldepflichten** kennt und über die **einzuhaltenden Fristen** Bescheid weiß?
- ☐ Sind die **Notfallkontakte** (z. B. Incident Responder, IT-Forensiker, Rechtsberatung) schnell erreichbar und griffbereit hinterlegt?
- ☐ Existiert eine geeignete (Cyber-) **Versicherung** und sind die Pflichten aus dem Versicherungsvertrag allen Verantwortlichen bekannt?
- ☐ Wurde eine **Urlaubsvertretung** organisiert und ist auch die **Wochenend-** und **Feiertagsbereitschaft** geregelt? (Achtung: Die Fristen bei meldepflichtigen Vorfällen sind auch während der Ferien, an Wochenenden und Feiertagen – z. B. in Österreich am 15. August – zu berücksichtigen!)
- ☐ Sind alle sicherheitsrelevanten Systeme auf dem neuesten Stand? (Sind die **aktuellen Updates** installiert? Sind die Firewalls richtig konfiguriert? Sind die Backups vollständig, sicher aufbewahrt und aktuell?)
- ☐ Und zu guter Letzt **das Wichtigste**: Wurde diese Checkliste **ausgedruckt** und **gut sichtbar** im Büro hinterlegt?

"Schoenherr takes a tactical and client-centric approach to challenges. It has creativity and the ability to think outside the box."

Chambers Europe

"Highly professional services. Always available as a trusted legal partner."

Legal 500

Cybernotfall – Checkliste im Fall eines Cyberangriffs / Cybervorfalls

Bereits beim **ersten Verdacht** eines Cyberangriffs bzw. Cybervorfalls gilt:

Unverzügliche Information der zuständigen Stellen:

- IT-Abteilung
- Chief Information Security Officer (CISO)
- Rechtsabteilung
- Datenschutzbeauftragte*r
- Rechtsvertretung
- Gegebenenfalls: Incident Response Team

Notfallkontakt

24/7-Notfall-E-Mail:
cyberincident@schoenherr.eu

Rasche Unterstützung bei:

Rechtlicher Ersteinschätzung der Situation, Übernahme von Meldepflichten und Abstimmungen mit Incident Respondern sowie IT-Forensikern, Prüfung von Regresspotenzialen und der Korrespondenz mit Behörden.

- ☐ **Sachverhaltserhebung:** Was ist genau geschehen? Ist der Angriff / Vorfall noch aktiv oder bereits beendet?
- ☐ **Dokumentation:** Sorgfältige Erfassung des Vorfalls und, sofern möglich, Sammlung forensisch verwertbarer Beweismittel – auch während laufender Wiederherstellungs- und Reparaturmaßnahmen.
- ☐ **Einschätzung der Lage:** Bewertung des Vorfalls hinsichtlich Ausmaßes, Schwere und potenzieller Folgen.
- ☐ **Versicherung benachrichtigen (sofern erforderlich):** Beachten Sie Meldepflichten sowie Obliegenheiten und greifen Sie gegebenenfalls auf angebotene Unterstützung zu.
- ☐ **Behördeninformation:**
  - Einhaltung gesetzlicher Meldefristen
  - Datenschutzbehörde: spätestens innerhalb von 72 Stunden
  - Unverzüglich im Rahmen des NISG
  - Gegebenenfalls Meldung an weitere Behörden (z. B. Polizei)
- ☐ **Sonderfall börsennotierte Unternehmen:** Zusätzliche Verpflichtungen beachten.
- ☐ **Information an externe Dritte / Öffentlichkeit (falls erforderlich):** Strategisch und rechtlich abgestimmt.
- ☐ **PR-Maßnahmen:** Kommunikation intern und extern sorgfältig vorbereiten.
- ☐ **Ruhe bewahren:** Überlegtes und koordiniertes Handeln ist entscheidend!

Weitere Informationen:
www.schoenherr.eu/cybersecurity