CYBERNOTFALL CHECKLISTE

Der Ernstfall ist eingetreten: Ihr Unternehmen wurde gehackt, Schadsoftware hat Ihr System infiltriert oder Sie werden von Cyberkriminellen erpresst? Sobald der Verdacht eines Cyberangriffs im Raum steht, sollten Sie erste Schritte einleiten. Wir haben 12 Maßnahmen für Sie zusammengestellt.

Sie sind unsicher, ob Sie gehackt wurden, oder nicht? Die CYBERsicher Notfallhilfe ist im Ernstfall für Sie da!

- Mithilfe eines Online-Selbstchecks können Sie bei der CYBERsicher Notfallhilfe den Sicherheitsvorfall unkompliziert einschätzen und passende Gegenmaßnahmen ergreifen.
- Sie erhalten eine auf den Vorfall zugeschnittene Übersicht der öffentlichen Anlaufstellen, wie etwa der Zentralen Ansprechstellen Cybercrime (ZAC).
- Falls Sie professionelle Unterstützung in Anspruch nehmen wollen, bietet die kostenfreie Plattform zudem die Möglichkeit, mit verfügbaren IT-Dienstleistern in Kontakt zu treten.

Schnell, unkompliziert, anonym!

- [ ] Bewahren Sie Ruhe und gehen Sie sehr überlegt vor. Es ist wichtig, dass der Vorfall rekonstruierbar bleibt und unüberlegte, stressbedingte Handlungen vermieden werden.
- [ ] Überprüfen Sie mithilfe der CYBERsicher Notfallhilfe, ob tatsächlich ein Sicherheitsvorfall vorliegt. Erhalten Sie konkrete Handlungsmaßnahmen und treten Sie bei Bedarf mit verfügbaren IT-Dienstleistern in Kontakt.
- [ ] Trennen Sie Ihr existierendes Backup-System physisch vom Netz (falls dadurch keine Daten o. ä. verloren gehen), um es vor einer Infizierung mit Schadsoftware zu schützen.
- [ ] Unternehmen ab einer bestimmten Größe sollten ein Team zusammenstellen, das alle relevanten Akteur:innen (Geschäftsleitung, IT-Administrator:innen, Datenschutzbeauftragte:r, Kommunikationsabteilung, ...) in den nächsten Schritten mit einbezieht. Legen Sie gemeinsam Aufgaben fest und vereinbaren Sie, wann die Runde wieder zusammentrifft.
- [ ] Isolieren Sie, falls gefahrlos möglich, Ihre betroffenen Systeme und ändern Sie schnellstmöglich die Passwörter der betroffenen Systeme oder Anwendungen.

CYBERsicher Transferstelle. Cybersicherheit. Mittelstand.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

- [ ] Falls personenbezogene Daten betroffen sind, müssen Sie innerhalb von 72 Std. die zuständige Aufsichtsbehörde (den Landesbeauftragten für Datenschutz und Informationsfreiheit Ihres Bundeslandes) über den Vorfall informieren.
- [ ] Informieren Sie Ihre betroffenen Kund:innen, Partner und Dienstleister direkt über den Vorfall, sodass diese vorgewarnt sind.
- [ ] Wenn Sie eine Cyberversicherung haben oder mit IT-Dienstleistern zusammenarbeiten, informieren Sie die Partner, um Unterstützung zu erhalten.
- [ ] Informieren Sie Ihre Mitarbeitenden über den Vorfall, mit der Bitte sich zu melden, falls sie etwas Merkwürdiges bemerkt haben. Versichern Sie ihnen, dass sie nicht bestraft werden, wenn sie einen Fehler begangen haben, um eine transparente Kommunikation zu ermutigen.
- [ ] Dokumentieren Sie den aktuellen Zustand und alle Änderungen an den Systemen (bspw. mit Handyfotos), um später den IT-Sicherheitsvorfall rekonstruieren zu können.
- [ ] Erstatten Sie, wenn nötig, eine Anzeige bei der Zentralen Ansprechstelle Cybercrime (ZAC) Ihres Landeskriminalamts.
- [ ] Gehen Sie keiner Lösegeldforderung nach und schicken Sie keine Daten an die Angreifer.

Wichtige Kontakte für den Notfall:

.....

.....

.....

.....

.....

www.transferstelle-cybersicherheit.de

Impressum | Der Mittelstand, BVMW e.V. | Potsdamer Str. 7 | 10785 Berlin
Vereinsregister Berlin Charlottenburg Nr. 19361 Nz | USt.-ID-Nr. DE 230883382

Weitere Materialien sowie Veranstaltungen und Angebote rund um das Thema Cybersicherheit finden Sie auf unserer Website.

Dort können Sie auch unseren Newsletter abonnieren, der Sie einmal pro Monat über alle aktuellen Angebote der Transferstelle Cybersicherheit im Mittelstand informiert.

Besuchen Sie unsere Website

CYBERsicher Transferstelle. Cybersicherheit. Mittelstand.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages