Zahlungsverkehr bei Cyber-Angriff sicherstellen

Stellen Sie sich vor, nichts geht mehr.

Ihr Unternehmen wird Opfer eines Cyberangriffes. Festnetztelefonie, Computer, E-Mail intern wie extern funktionieren nicht mehr. Ihre Daten sind verschlüsselt und nicht mehr abrufbar. Ihre IT inkl. Geschäftsprozesse kommen zum Erliegen. Sie haben keinen Internetzugang und kein WLAN mehr. Und zu guter Letzt: Dringende Zahlungen stehen an, wie z.B. Gehälter, Versicherungen etc.

Haben Sie einen Notfallplan?

Je besser Ihre Notfallpläne sind, desto handlungsfähiger sind Sie. **Und drucken Sie Ihren Notfallplan aus.** In Bezug auf Ihren Zahlungsverkehr unterstützen wir Sie als Commerzbank sowohl im Vorfeld als auch im akuten Notfall.

Vorbereitungen für den Notfall:

1. Für den Fall, dass Ihre Firmentelefonie (Mobil, Festnetz) oder E-Mail nicht mehr funktionieren, können Sie vorab bei Ihrem Firmenkundenbetreuer alternative Kontaktdaten (z.B. Handy-Nummern oder E-Mail-Adressen) der Bank-Bevollmächtigten im Unternehmen hinterlegen. Dies erleichtert dem Bankbetreuer z.B. die Identifizierung des Anrufers mit einer anderen Nummer.
2. Bereiten Sie eine Notfallliste mit allen relevanten Kontaktinformationen Ihrer internen und externen Ansprechpartner vor und drucken Sie sie aus.
3. Implementieren Sie für Ihren Zahlungsverkehr ein webbasiertes Tool als Backup und testen Sie dieses vorab. Loggen Sie sich regelmäßig alle 3 oder 6 Monate ein, damit Ihr Zugang nicht wegen Inaktivität deaktiviert wird. Und erstellen Sie regelmäßig Backups Ihrer Zahlungsverkehrsdaten, z.B. auf einem USB-Stick, damit Sie im Notfall die nötigen Datensätze nicht manuell neu erfassen müssen.
4. Versorgen Sie sich im Vorfeld mit photoTAN-Lesegeräten, für den Fall, dass die photoTAN-App auf mobilen Firmengeräten ausfallen sollte.
5. Führen Sie regelmäßig Awareness-Trainings für Mitarbeiter im Unternehmen durch. Und tauschen Sie sich regelmäßig im Management/Team über aktuelle Angriffsversuche und insbesondere der Phishing-Varianten aus, denn über 90% der Angriffe beginnen mit Phishing.

Weitere Präventionsangebote der Commerzbank:

Implementieren Sie für Ihren Zahlungsverkehr und Ihr Cash Management ein webbasiertes Tool als Backup, wie z.B. Global Payment Plus oder unser Treasury Management System mit Datenhaltung in der Commerzbank-Cloud.

Wenn Sie Unterstützung bei einer Cyberversicherung oder Cyber- und IT-Sicherheitsberatung benötigen, sprechen Sie uns an. Wir arbeiten hier mit ausgewählten geprüften Kooperationspartnern zusammen und vermitteln Ihnen gerne passende Ansprechpartner.

Sprechen Sie uns an. Wir unterstützen Sie gerne.

Was tun im Notfall?

- ☑ Erstmal Ruhe bewahren.
- ☑ Rufen Sie Ihren Firmenkundenbetreuer an und schildern Sie ihm die Umstände so detailliert wie möglich.
- ☑ Sofern möglich, verschaffen Sie sich einen Überblick über aktuelle Buchungsvorgänge oder Auszüge.
- ☑ Wenn kurzfristig wichtige Zahlungen anstehen, wie z.B. Gehälter, Versicherungen, informieren Sie uns bitte rechtzeitig, wenn die Abwicklung über Ihre Bankingsysteme nicht mehr sichergestellt ist.
- ☑ Wir verfügen über Kontakte zur Polizei und Forensikern und können hier bei Bedarf unterstützen.
- ☑ Wenn Sie Konten, Karten oder Zugänge/Berechtigungen sperren lassen möchten, nutzen Sie unsere Hotlines oder sprechen Sie Ihren Firmenkundenbetreuer an.

Hotlines als Kontaktmöglichkeiten | Kontakt - Commerzbank

Produkt-spezifische Hotlines		
Firmenkunden-Hotline	*Mo. - Fr.: 8.00 bis 18.00 Uhr*	+49 69 136 263 60
Corporate-Card-Service-Hotline	*Täglich rund um die Uhr*	+49 69 5050 2785
Point-of-Sale-Service-Hotline	*Mo. bis Fr.: 7.30 bis 20.30 Uhr, Sa.: 8.00 bis 16.30 Uhr*	+49 69 5050 2787
Web-Point-of-Sale-Service-Hotline	*Mo. bis Fr.: 7.30 bis 20.30 Uhr, Sa.: 8.00 bis 16.30 Uhr*	+49 69 5050 2784
HBCI/StarMoney-Hotline	*Mo. - Fr.: 7.00 bis 19.00 Uhr*	+49 69 9866 0022
Notfall- und Sperrhotlines		
Kartensperrservice Corporate Card	*Täglich rund um die Uhr*	+49 69 5050 2040
Sperrhotline Firmenkundenportal	*Täglich rund um die Uhr*	+49 69 5050 2786
Notfall-Hotline für Kartenversicherung Corporate Card	*Täglich rund um die Uhr*	+49 89 624 245 63

Weitere Informationen vom Bundesamt für Sicherheit in der Informationstechnik finden Sie hier:
BSI – Ransomware 1. Hilfe bei einem schwerem IT-Sicherheitsvorfall
BSI – Maßnahmenkatalog zum Notfallmanagement