BADEN CLOUD
Die Zukunft Ihrer Daten

Powered by

LEITWERK

E-Werk Mittelbaden

Cyberangriff und ihre wirtschaftlichen Folgen!

Was Unternehmen umgehend prüfen sollten, um für einen Cybervorfall besser gewappnet zu sein.

www.badencloud.de

BADEN CLOUD
Die Zukunft Ihrer Daten

Cyberangriff und ihre wirtschaftlichen Folgen!

Was Unternehmen umgehend prüfen sollten, um für einen Cybervorfall besser gewappnet zu sein.

Ein einzelner unbedachter Mausklick reicht bereits aus, um Opfer von Cyberkriminalität zu werden. Als besonders heimtückisch entpuppen sich seit Ende 2018 die Verschlüsselungstrojaner der neuesten Generation. So gehen Verschlüsselungstrojaner wie Emotet und Grandcrab mit äußerst ausgeklügelten Angriffstechniken gezielt gegen Unternehmen aller Branchen und Größen vor. Die Erpressungsforderungen sind dabei angepasst an den jeweiligen Unternehmensumsatz. Laut BSI (Bundesamt für Sicherheit in der Informationstechnik) drohen existenzbedrohende Datenverluste.

Beginnen Sie Ihre Schutzmaßnahmen, indem Sie sich vor Augen führen: **„Cyberangriffe können auch uns treffen "** und schaffen Sie hierfür das nötige Bewusstsein in Ihrem Unternehmen und bei Ihren Usern.

Denn: Der User ist und bleibt der größte Risikofaktor!

Sie möchten Ihre Risiken genauer kennenlernen und dringend erforderliche Schutzmaßnahmen möglichst schnell umsetzen?

Dann sprechen Sie uns an! (support@leitwerk.de) Wir prüfen Ihre IT-Umgebung in den für Ransomware anfälligsten Bereichen und geben Ihnen Tipps und Hinweise auf mögliche Verbesserungen. Unsere Prüfmethodik umfasst neben der Firewall-Umgebung und den Remote-Zugängen die Bereiche Backup, Patch-Management, Virenschutz und Netzwerksegmentierung.

BADEN CLOUD
Die Zukunft Ihrer Daten

Ob gemeinsam mit unseren Security-Experten effizient im Rahmen des „Security Checks“ oder mit den geeigneten Experten in Ihrem Unternehmen – stellen Sie sich vor dem Hintergrund der aktuellen Gefährdungslage folgende Fragen (ohne Anspruch auf Vollständigkeit). Die Auswertung der nachstehenden Liste ist die Grundlage, um die spezifische Gefährdung für Ihr Unternehmen zu bewerten:

Bereich Firewall/Remote-Zugänge

- Sind aktuelle Schutzmaßnahmen (z.B. IPS, Applikationskontrolle, HTTPs-Scan, Sandboxing) aktiviert?
- Sind Zugriffe von extern abgesichert?
- Wie sind diese abgesichert?
- Sind Makros in Office-Dokumenten generell inaktiv?
- Werden alte Dateiformate blockiert?

Bereich Backup

- Ist das Backup-System in der Domäne?
- Welche Personen haben Zugriff auf Ihr System?
- Wie oft sichern Sie Ihre Daten?
- Sind Zugriffe auf die Backups aus dem produktiven Netzwerk möglich?
- Sind die Backups zusätzlich abgesichert?
- Sind aktuelle Sicherungen außerhalb des Unternehmens (beispielsweise auf Magnetbändern) vorhanden?
- Sind Wiederherstellungen bereits durchgeführt oder getestet worden?
- Sind Ihre Backups wiederherstellbar?
- Wie lange dauert eine komplette Rücksicherung?

Bereich Patch Management

- Existiert ein durchgängiges Patch Management?
- Wie wird Software (nicht nur Microsoft!) aktuell gehalten?
- Wird regelmäßig die Aktualität der Updates überprüft?

Bereich Virenschutz

- Ist der Virenscanner immer aktuell?
- Ist der Virenscanner mit aktuellen Überprüfungsmethoden ausgestattet und sind diese aktiv (z.B. Verhaltensüberwachung)?
- Befinden sich alle Systeme auf dem aktuellen Stand und werden sie vom Hersteller noch unterstützt?

Bereich Netzwerk/Segmentierung

- Sind bestimmte Netzwerkbereiche isoliert bzw. reglementiert aufgrund von Risikobewertungen?
- Sind Produktionsmaschinen isoliert bzw. separiert?
- Sind Zugriffesrechte auf das erforderliche Minimum reduziert?

BADEN CLOUD
Die Zukunft Ihrer Daten

Neben den genannten technischen Fragestellungen sollten Sie außerdem organisatorische Maßnahmen, den Datenschutz sowie Compliance-Themen stets im Blick behalten, z.B.:

- Ist ein Datenschutzbeauftragter benannt?
- Wird das Thema Datenschutz in Ihrem Unternehmen DSGVO-konform betrieben?
- Wird Informationssicherheit nach BSI-Standard betrieben?
- Gibt es einen IT-Notfallplan sowie Vorbereitungen für ein Krisenmanagement?
- Berücksichtigen Sie die neuen Anforderungen nach Überarbeitung des Geschäftsgeheimnisgesetz im Mai 2019?

Erfahren Sie in einem persönlichen Gespräch weitere Details und welche Schritte Sie einleiten sollten, um sich ausreichend zu schützen. Vereinbaren Sie noch heute einen Termin.

Ihr Ansprechpartner

Marco Andreano
Technische Leitung, ppa.
E-Mail: mandreano@leitwerk.de

Thomas Heß
Leitung Cyberangriff Taskforce
E-Mail: thess@leitwerk.de

BADEN CLOUD®
Im Ettenbach 13a | 77767 Appenweier-Urloffen
Tel.: +49 7805 918 - 0 | info@badencloud.de | www.badencloud.de