TREUHAND | SUISSE
Schweizerischer Treuhänderverband

Cybersecurity im Treuhandunternehmen

I. Cybersecurity

Cyberangriffe können auch Ihr Unternehmen treffen. Kein Unternehmen, das die Vorteile der Digitalisierung nutzt, kommt heute um das Thema Cybersicherheit herum. Die Verantwortung zum Eigenschutz liegt beim jeweiligen Unternehmen. Risikopotential und -ausmass von Cyberangriffen lassen sich mit organisatorischen und technischen Massnahmen minimieren. Mit organisatorischen Massnahmen lässt sich die Informationssicherheit, mit technischen Massnahmen die Sicherheit der ICT-Infrastruktur erhöhen. Beide Arten von Massnahmen müssen sich ergänzen, um einen adäquaten Schutz des Unternehmens zu erreichen.

Mögliche Cyberbedrohungen sind beispielsweise Angriffe auf die Verfügbarkeit von Systemen (DDoS), Ransomware („Verschlüsselungstrojaner"), Phishing, Datenabfluss, CEO-Fraud, Rechnungsmanipulationsbetrug (BEC-Fraud), Hacking oder Domänenregistrierungsbetrug.

II. Cybersecurity-Schnelltest und Leitfaden für KMU

Der Bund und verschiedenen Organisationen[1] haben gemeinsam den Cybersecurity-Schnelltest für KMU entwickelt, mit dem Unternehmen testen können, wie gut sie vor Angriffen aus dem Cyberspace geschützt sind und ob sie die Minimalstandards für KMU erfüllen.

Mit dem Schnelltest können KMU herausfinden, ob ihre technischen, organisatorischen und mitarbeiterbezogenen Massnahmen ausreichend Schutz vor Cyber-Risiken bieten. Der Test bietet keine umfassende und vollständige Analyse. Er dient aber KMU, insbesondere solchen mit wenig Know-how über ICT und Cybersicherheit, als Standortbestimmung, indem er die wesentlichen Fragen, mit denen sich ein Unternehmen befassen muss, stellt. Die Fragen können sowohl online als auch offline beantwortet werden.

Unter www.cybersecurity-check.ch finden Sie den Schnelltest und den ergänzenden Cybersecurity-Leitfaden für KMU, der Unternehmen eine Hilfestellung bietet, wie eine minimale Cybersecurity und damit ein erhöhter Schutz vor den häufigsten Cyberattacken erreicht werden kann. Der Leitfaden behandelt die folgenden Themen: Sicherheit im Bereich Organisation und Prozesse, Sicherheit dank dem Faktor Mensch, Sicherheit dank geeigneter technischer Massnahmen, Cybersicherheit als Teil des Datenschutzes und Sicherheit dank geeignetem Umfeld. In jedem Thema wird in kurzer Form erklärt, weshalb es wichtig ist, was getan werden kann und wie vorzugehen ist.

III. Nationales Zentrum für Cybersicherheit (NCSC)

Das Nationale Zentrum für Cybersicherheit (National Cyber Security Centre, NCSC) ist das Kompetenzzentrum des Bundes für Cybersicherheit. Es ist erste Anlaufstelle für die Wirtschaft, die Verwaltung, für Bildungseinrichtungen und die Bevölkerung bei Cyberfragen. Seine Melde- und Analysestelle Informationssicherung (MELANI) beinhaltet die neu geschaffene Nationale Anlaufstelle, die Meldungen zu Cybervorfällen aus der Bevölkerung und der Wirtschaft entgegennimmt, analysiert und den Meldenden eine Einschätzung zum Vorfall mit Empfehlungen für das weitere Vorgehen gibt.

Das NCSC stellt umfangreiche Informationen zur Cybersicherheit unter anderem für Unternehmen zur Verfügung (www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen.html).

[1] dititalswitzerland, ISSS, satw, SNV, SQS und ASA/SVV

Zurzeit finden sich Informationen und Hinweise zu präventiven Massnahmen zu folgenden aktuellen Themen auf der Webseite des NCSC:

- Cyberangriffe gegen Firmen - Das müssen Sie wissen
- Empfehlungen für die Zusammenarbeit mit IT-Providern
- Home Office - Sicherer Umgang mit Fernzugriffen
- IKT-Minimalstandards
- Massnahmen zum Schutz von CMS
- Massnahmen zum Schutz von ICS
- Massnahmen zum Schutz von IOT Geräten
- Massnahmen zum Schutz vor DDoS-Angriffen
- Reisen ins Ausland
- Schützen Sie Ihre Konten/Passwörter
- Schützen Sie Ihr KMU
- Verhalten bei E-Mail
- Zahlungsprozesse im Griff?

Auch für den Fall, dass ein Cybervorfall eingetreten ist, bietet das NCSC Informationen und Hilfestellungen:

- Ransomware - Was nun?
- Webseite gehackt - Was nun?
- Datenabfluss - Was nun?
- Cyberattacke - Was tun? Checkliste für CISOs
- DDoS-Angriff - Was nun?

Über ein Webformular können sodann Cybervorfälle oder Schwachstellen unkompliziert online gemeldet werden.

IV. Cyberrisiko-Versicherungen

Cyberrisiken haben im Geschäftsalltag an Bedeutung gewonnen und die Risikolage erhöht sich ständig. Daher hat die Versicherungsbranche spezielle Cyberrisiko-Versicherungen entwickelt. Unternehmen können mit solchen Versicherungen wesentliche Komponenten ihres Risikos versichern. Die Cyberrisiko-Versicherungen bestehen in der Regel aus verschiedenen Bausteinen, aber nicht jeder Versicherer bietet unter dem gleichen Baustein den gleichen Schutz. Es empfiehlt sich daher, verschiedene Versicherungslösungen auf der Basis einer Analyse des unternehmensspezifischen Risikos resp. Versicherungsbedürfnisses zu vergleichen und mit den bestehenden Versicherungspolicen abzustimmen, um sowohl Deckungslücken als auch Doppelversicherungen zu vermeiden.

V. Angebot und Unterstützung von TREUHAND|SUISSE

TREUHAND|SUISSE trägt dem Thema Cybersecurity im Treuhandunternehmen Rechnung und schafft für seine Mitglieder ab Frühsommer 2022 eine zentrale Anlaufstelle für alle Fragen rund um diese Problematik. Neben generellen Sicherheitsinformationen werden unter anderem Publikationen zur Sensibilisierung der Mitarbeitenden veröffentlicht, Möglichkeiten aufgezeigt, wie ein Unternehmen seine Cybersicherheit testen lassen kann, und Hilfestellungen für die Erlangung eines optimalen Schutzes geboten.

Wir halten Sie auf dem Laufenden. Abonnieren Sie auf den sozialen Medien auch die Beiträge des Instituts Treuhand 4.0, um stets informiert zu sein über aktuelle Cybersecurity-Themen.