Leitfaden für IT-Security *(Datenschutz)*

Ein Produkt vom Institut Treuhand 4.0 von TREUHAND|SUISSE

Stand: 29. Juli 2020 - Version 1.0

Inhalt

Einleitung

Dieser Leitfaden richtet sich an die Mitglieder von TREUHAND|SUISSE und allen interessierten Schweizer KMU's. Das Dokument soll ihnen dabei helfen ihre IT-Security zu analysieren und die nötigen Massnahmen zu treffen, um die Informationssicherheit in ihrer Systemlandschaft und im Unternehmensnetzwerk zu erhöhen.
Der Leitfaden gliedert sich in verschiedene Schutzmassnahmen, die als Empfehlung analysiert und bei Bedarf optimiert werden können.

Schutzmassnahmen

Schutz durch geeignete Organisation und Prozesse

Worum geht es?

Bei einem Cyber-Vorfall ist die kurze Reaktionszeit ein Schlüsselelement. Aus diesem Grund müssen die nötigen organisatorischen Massnahmen im Vorfeld getroffen sein, um bei Bedarf schnell und zielführend reagieren zu können.

Welche Massnahmen sollte ich treffen - Wie ist das Vorgehen?

Organisatorisch müssen die Risiken soweit erkannt und Lösungen vorhanden sein, um einen möglichst unterbrechungsfreien Betrieb zu gewährleisten - Die Arbeiten müssen auch erledigt werden können, wenn die IT komplett oder teilweise nicht mehr funktioniert. Dies als Folge eines Cyber-Angriffs aber auch durch Stromausfälle, Internetausfälle, Brände, etc.. Hierzu sollten alternative Lösungen oder Backup-Systeme frühzeitig ins Auge gefasst werden.

Evaluation der Abhängigkeiten der Geschäftsprozesse von der IT-Infrastruktur - Wie sind die Auswirkungen bei fehlendem Zugriff auf Daten oder dem Ausfall eines Systems? Was für Massnahmen kann ich zur Prävention ergreifen?

Definition eines Verantwortlichen für IT-Security - Alle Mitarbeitenden müssen genau wissen, an wen sie sich bei Fragen zur Sicherheit (z.B. beim Erhalt eines verdächtigen E-Mails von einem Kunden) oder bei einem Sicherheitsvorfall wenden können.

Definition der Zuständigkeit zwischen dem Unternehmen und dem IT-Dienstleister betreffend IT-Security – Wenn sicherheitsrelevante Dienstleistungen (z.B. Backup) ausgelagert werden, muss regelmässig kontrolliert werden, dass die Massnahmen korrekt umgesetzt werden. Die entsprechend Dienstleistungsverträge sollten keine Missverständnisse zulassen und alle Verantwortlichkeiten müssen klar definiert sein.

Erstellen eines Notfallplanes – Der vorbereitete Notfallplan leitet die verantwortliche Person bei einem Vorfall sauber durch die vordefinierten Tasks. Hier sollten Punkte abgehandelt werden, wie die

Identifikation der kritischen System (z.B. Mail, CRM, Buchhaltungsmandanten, Steuerdaten, etc.), vorbereitete Rückfallsysteme (z.B. Ersatz Infrastruktur oder die Vorplanung einer effizienten Ersatzbeschaffung), Definition genauer Vorgehen (z.B. Client vom Netz bei Virusverdacht) oder klare Definition einer nötigen Systemwiederherstellung.

Schutz durch Einbezug der Mitarbeitenden (Faktor Mensch)

Worum geht es?

Alle möglichen technischen Hilfestellungen nützen nichts, wenn die Mitarbeitenden in die IT-Security nicht miteinbezogen werden. Es ist unerlässlich, die Mitarbeitenden über aktuelle Gefahren zu informieren und die wichtigsten Regeln zu deren Verhalten klar zu definieren.

Welche Massnahmen sollte ich treffen - Wie ist das Vorgehen?

Schulung der Mitarbeitenden – die Mitarbeitenden sollten fortlaufend auf IT-Security im Geschäftsalltag aufmerksam gemacht werden und es muss ihnen aufgezeigt werden, wo mögliche Probleme/Fehler bei der Verwendung vom Internet, E-Mail und generell der IT-Infrastruktur auftreten können. Es empfiehlt sich, den Mitarbeitenden eine Basisausbildung zu Themen wie der Nutzen der IT-Security, Passwörter und sicherer Umgang mit Internet und E-Mail anzubieten.

Definieren einer Passwort-Policy – Für das Unternehmen sollten verbindliche Passwortregeln für sichere Passwörter definiert werden. Wo immer möglich sollte eine Zwei-Faktor Authentisierung verwendet werden. Als Hilfestellung kann den Mitarbeitenden auch aufgezeigt werden, wie mit Hilfe einer Eselsleiter komplexe Passwörter gemerkt werden können.

Schutz durch Massnahmen auf der technischen Ebene

Worum geht es?

Eine absolute Sicherheit erreicht man auch durch die technischen Massnahmen nicht. Jedoch können durch Sicherheitslücken Unbefugte auf Ihr System oder in Ihr Netzwerk eindringen und Daten vernichten oder manipulieren. Die von den Herstellern zur Verfügung gestellten Sicherheitsupdates schliessen bekannte Sicherheitslücken. Wenn ein Datenverkehr ausserhalb des Firmennetzwerk nicht verschlüsselt wird, kann dieser mitgelesen oder sogar manipuliert werden.

Welche Massnahmen sollte ich treffen - Wie ist das Vorgehen?

Planen eines Backups – Um dem Verlust von Daten vorzubeugen, muss mindestens wöchentlich ein Backup auf einen externen Datenträger gesichert werden, welcher extern an einem geschützten Ort gelagert wird. Es soll offline sein, d.h. nicht im Netzwerk. Wichtig ist auch ein regelmässiger Test, ob die Daten aus dem Backup zurückgespielt werden können

Einsatz eines Virenschutzes – Auf allen Clients und Servern soll ein aktueller Virenschutz installiert sein, welcher regelmässig aktualisiert wird und vollständige Systemscans durchführt.

Regelmässige Aktualisierung der eingesetzten Anwendungen – Veraltete Applikationen ist das Einfallstor für Schadsoftware. Stellen Sie sicher, dass sämtliche Computer, Server, NAS, Firewalls, etc. im Netzwerk die vorhandenen Sicherheitsupdates, wenn möglich automatisch oder zeitnah nach vorgängiger Prüfung möglichst schnell eingespielt werden. Alte Geräte, für die keine Sicherheitsupdates mehr verfügbar sind, dürfen nicht mit dem Firmennetzwerk verbunden werden.

Einsatz von Firewalls – Jeder eingesetzte Computer sollte eine aktive Firewall haben. Weiter sollte das Unternehmensnetzwerk gegenüber dem Internet durch eine zusätzliche Firewall geschützt werden. Der korrekten Konfiguration der Firewall sollte eine grosse Aufmerksamkeit geschenkt werden, sowie deren regelmässigen Aktualisierung mit Updates.

Einsatz von Spam-Filtern – Spam-E-Mails sollten durch den Einsatz von geeigneten Tools und Konfigurationen blockiert werden. So können generell E-Mails aus gewissen Ländern blockiert werden oder potentiell schädliche Anhänge in E-Mails bereits durch den E-Mail-Gateway oder den Spam-Filter gefiltert werden.

Implementierung einer Netzwerksegmentierung – Computer der Steuerabteilung, der Buchhaltung und dem HR sollten in einem separaten Netzwerk sein, sodass diese untereinander nicht erreicht werden können. Auch beim Einsatz von Netzwerk-Shares ist Vorsicht geboten, da sich darüber auch Malware verbreiten kann. Fragen Sie hierzu Ihren IT-Dienstleister.

Deaktivieren der Makros – Diese Funktion wird verwendet, um Office-Dokumente zu automatisieren. Leider werden die Makros immer öfters dazu verwendet, um Schadsoftware zu verbreiten. Das neue Format von Microsoft (z.B. docx) enthält keine Makros. Hier empfiehlt es sich, mit aktuellen Microsoft-Produkten zu arbeiten, die die neuen Formate unterstützen.

Sichern von extern Zugriffen – Wenn Mitarbeitende von unterwegs auf das Firmennetzwerk zugreifen müssen, muss sichergestellt werden, dass ein Remote-Zugang (z.B. RAS, VPN) verwendet wird, welcher eine starke Authentifizierung erfordert, idealerweise eine Zwei-Faktoren-Authentifizierung.

Schützen des Content Management Systems – beim Vorhandensein eines Internetauftritts unter Mitwirkung eines CMS sollte sichergestellt werden, dass dies auch auf dem neusten Stand ist.

Datenschutz

Worum geht es?

Jedes Unternehmen ist verantwortlich für den sicheren Umgang mit Personendaten und geistigem Eigentum. Bei Datenverlust oder Datenschutzverletzungen drohen strafrechtliche Folgen, hohe Geldstrafen und schwerwiegender Imageverlust.
Seit 2018 ist die neue Datenschutzverordnung (DSGVO) der EU in Kraft, welche auch teilweise für Schweizer Unternehmen gilt.
Der Datenschutz hängt direkt auch von der IT-Security ab, da Kriminelle an sensible Daten gelangen können.

Welche Massnahmen sollte ich treffen - Wie ist das Vorgehen?

Gesetzeskonformer Umgang mit Daten – Bei allen Arbeiten mit Kundendaten (Beschaffung, Speicherung, Aufbewahrung, Verwendung, Veränderung, Archivierung und Löschung) müssen diese hinreichen geschützt werden.
Für die korrekte Umsetzung der DSGVO für Ihre Internetseite unter Berücksichtigung des Schweizer Rechts konsultieren Sie auch unseren Praxisguide.

Schutz durch Einbezug des Umfeldes

Worum geht es?

Wenn der Outsourcing-Partner, Lieferant oder Dienstleister von einem Hackerangriff betroffen ist, kann dies auch Ihr Unternehmen direkt betreffen. Aus diesem Grund ist es wichtig, dass die wichtigsten Massnahmen zur IT-Security auch durch diese Unternehmen umgesetzt werden.
Werden Dienstleistungen an einen externen Dienstleister ausgelagert, ist eine genaue Kontrolle notwendig.

Welche Massnahmen sollte ich treffen - Wie ist das Vorgehen?

Sicherheit in Bezug auf Cloud-Dienste – Der grosse Vorteil von Cloud-Diensten ist, dass keine teuren IT-Infrastrukturen betrieben werden müssen. Dies ist auch der Grund, dass sich solche Cloud-Dienste grosser Beliebtheit erfreuen. Jedoch entlässt Sie deren Verwendung nicht aus der Verantwortung der IT-Security. So sollte genau geprüft werden, wo sensible Daten abgelegt werden und wie diese umfassend geschützt werden können. Auch sollte vor Abschluss eines Vertrages mit einem Cloud-Dienstleister geprüft werden, wer alles Zugriff auf die Daten hat, wo die Datenhoheit liegt, wie die Datensicherung geregelt ist, etc.

Prüfungen beim Auslagern von IT-Security Dienstleistungen – Vor der Zusammenarbeit mit einem solchen Dienstleister sollte auf Zertifikate und die Einhaltung der IT-Sicherheitsmassnahmen Wert gelegt werden und entsprechende Nachweise eingefordert werden.

Prüfen der IT-Security des Dienstleisters und des Lieferanten – Stellen Sie sicher, dass die Anforderungen an die Sicherheit, welche für Ihr Unternehmen gestellt werden, auch von Ihrem Umfeld abgedeckt wird. Dies kann z.B. Backupregelung, Vorhandensein eines Notfallplanes, Einhalten von Benutzerrichtlinien, Vorgaben für Benutzeradministration, etc. betreffen.

Checkliste

Massnahme	Ja	Nein	weiss nicht
Schutz durch geeignete Organisation und Prozesse			
Organisatorische Risikoerkennung			
Evaluation der Abhängigkeit der Geschäftsprozesse			
Definition des Verantwortlichen für die IT-Security			
Definition der Zuständigkeit zwischen Unternehmen und externen IT-Dienstleistern			
Erstellen eines Notfallplans			
Schutz durch Einbezug der Mitarbeitenden (Faktor Mensch)			
Schulung der Mitarbeitenden			
Definieren einer Passwort-Policy			
Schutz durch Massnahmen auf der technischen Ebene			
Planen eines Backups			
Einsatz eines Virenschutzes			
Regelmässige Aktualisierung der eingesetzten Anwendungen			
Einsatz von Firewalls			
Einsatz von Spam-Filtern			
Implementierung einer Netzwerksegmentierung			
Deaktivieren der Makros			
Sichern von externen Zugriffen			
Schützen des Content Management Systems			
Datenschutz			
Gesetzeskonformer Umgang mit Daten			
Schutz durch Einbezug des Umfeldes			
Sicherheit in Bezug auf Cloud-Dienste			
Prüfungen beim Auslagern von IT-Security Dienstleistungen			
Prüfen der IT-Security des Dienstleisters und des Lieferanten			

Alle Massnahmen, die mit Nein oder weiss nicht versehen wurden bedürfen eines speziellen Augenmerks. Konsultieren Sie hierzu Ihren IT-Dienstleister oder fragen Sie uns, wir helfen Ihnen gerne weiter.

Schlusswort / Disclaimer

Dieser Leitfaden hat keinen Anspruch auf Vollständigkeit. Das Dokument ist primär als Anhaltspunkt zur Erarbeitung eines eigenen IT-Security-Konzeptes gedacht, um die eigene Infrastruktur im Unternehmen zu schützen unter Einbezug der Mitarbeitenden. Denn durch die gewissenhafte Information an die Mitarbeitenden kann bereits eine grosse Vorarbeit geleistet werden. Die technischen und konzeptionellen Vorkehrungen können noch so gut sein, wenn dem Faktor Mensch im Unternehmen nicht die benötigte Aufmerksamkeit geschenkt wird.
Je nach Geschäftsumfeld und Komplexität der IT-Infrastruktur kann parallel zur Umsetzung der eigenen IT-Security eine Cyberrisk-Versicherung geprüft werden.
Das Institut Treuhand 4.0 hat diesen Leitfaden mit der grössten Sorgfalt und im Bemühen um Korrektheit der Inhalte im Zeitpunkt der Veröffentlichung verfasst. Der Leitfaden ersetzt nicht die fachliche Beratung im Einzelfall und Adaption auf die konkrete Situation. Vollständigkeit und Richtigkeit werden nicht garantiert. Das Institut Treuhand 4.0 ist nicht verpflichtet, den Leitfaden zu aktualisieren und nachzuführen. Es übernimmt keine Haftung für allfällige Schäden, die aus der Verwendung dieses Leitfadens entstehen.

Weiterführende Informationen/Nachweise

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
Melde- und Analysestelle Informationssicherung MELANI
ICTswitzerland
Merkblatt für IT-Sicherheit - MELANI
Informationssicherheit im KMU – KMU Portal