GEOINFO
IT-SOLUTIONS

IT-SECURITY

EIN SECHS-PUNKTE-CHECK

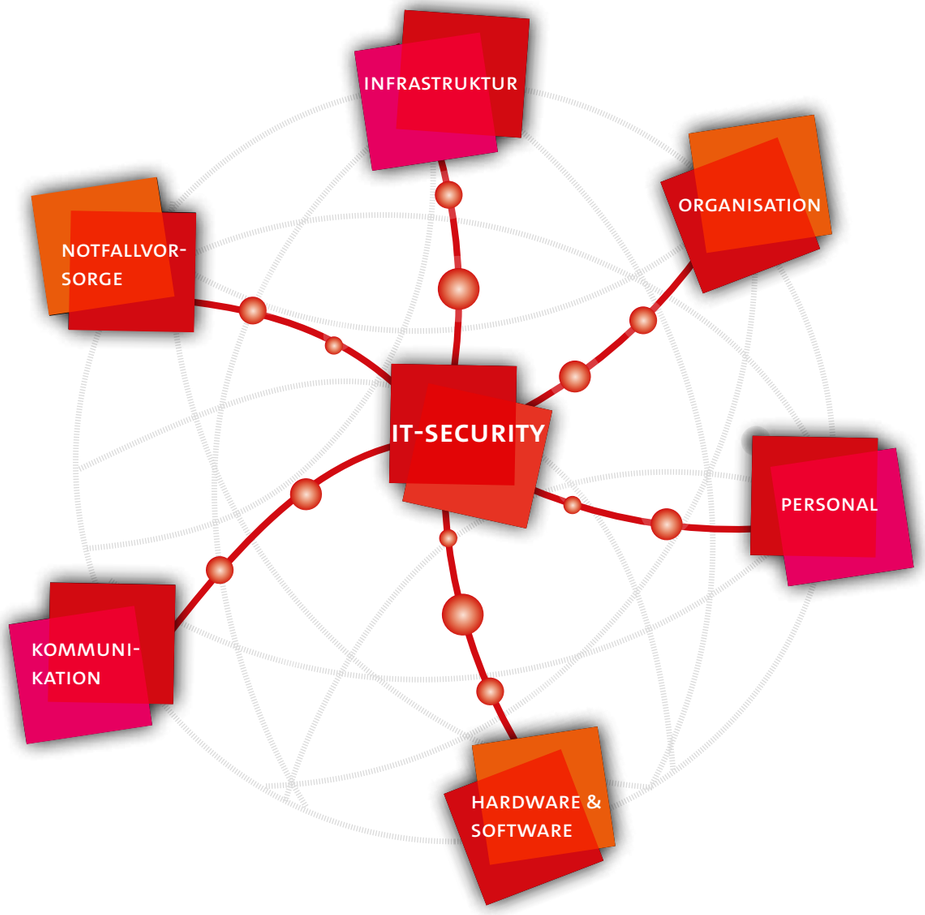
IT-Security: ein Sechs-Punkte-Check

Diese Checkliste *) richtet sich an kleine und mittlere Unternehmen (KMU) sowie Non-Profit-Organisationen (NPO). Sie gliedert sich in sechs Themenbereiche und soll helfen, die IT-Sicherheit im Unternehmen zu erhöhen. Dieser wichtige Aspekt der Unternehmensführung wird häufig vernachlässigt.

Cybercrime trifft auch KMU
Cybercrime trifft nicht nur Grossunternehmen. Auch für KMU und NPO nimmt die Bedrohung stetig zu. Alleine schon der verursachte Reputationsschaden kann die Existenz ernsthaft bedrohen.

Ganz unabhängig von der Unternehmensgrösse: Nur gut aufeinander abgestimmte technische und organisatorische Massnahmen gewährleisten eine hohe IT-Sicherheit. Ein Restrisiko bleibt immer bestehen. Es gilt, die Sicherheitskosten gegen potenzielle Schadenszenarien abzuwägen. Unsere erfahrenen IT-Fachleute unterstützen diesen Prozess.

*) Behandelt werden die aus unserer Sicht wichtigsten Punkte. Als Basis dient der Massnahmenkatalog des IT-Grundschutzes des Deutschen Bundesamts für Sicherheit in der Informationstechnik, der gilt als Branchenstandard gilt.



1. Die Infrastruktur

Die IT-Infrastruktur regelt über diverse Schnittstellen den Zugriff für berechtigte Mitarbeitende und Kunden. Diese Zugänge sind laufend auf mögliche Datenlecks zu überprüfen, inklusive aller Mobilgeräte.

Zugang einschränken
Es gilt zu definieren, welche Bereiche im Unternehmen schützenswert sind. Dazu zählt zum Beispiel der Serverraum. Dieser darf nur Berechtigten zugänglich sein.

Auch die Verkabelung kann mit entsprechenden technischen Mitteln als Angriffspunkt dienen. Sie ist darum ebenfalls zu schützen und zusammen mit kabellosen Netzwerken bei der Massnahmenplanung zu berücksichtigen.

Mobile Arbeitsgeräte sichern
Mobile Arbeitsplätze müssen vergleichbar hohen Sicherheitsstandards genügen wie Büroräume im Firmengebäude.

Der Wert der gespeicherten Daten auf mobilen Geräten ist oft höher als der Materialwert des Geräts. Ohne spezielle Sicherheitsvorkehrungen wie z.B. der Datenverschlüsselung dürfen deshalb auf mobilen Geräten keine vertraulichen Daten gespeichert werden.

Mit einer internen Weisung ist zudem zu regeln, dass der Verlust eines mobilen Arbeitsgeräts umgehend der zuständigen Stelle zu melden ist.

Systemrelevante Komponenten überwachen
Ein Monitoring aller systemrelevanten Komponenten kann frühzeitig vor sich abzeichnenden Ausfällen warnen. Unsere Erfahrung zeigt, dass gerade KMU und NPO diesem Punkt oft zu wenig Bedeutung beimessen. Oft entscheiden wenige Stunden darüber, ob Daten verloren gehen oder nicht. Mit einem umfassenden Monitoring-System erkennen die IT-Verantwortlichen Störungen frühzeitig und können so bei Ausfällen rechtzeitig reagieren.

Zu überwachen ist die ganze Hardware wie Server, Speichersysteme, Firewalls, Switches, die unterbrechungsfreie Stromversorgung USV sowie die Telefonanlage. Wichtige Prozesse und Softwarekomponenten sollen ebenfalls überwacht werden. Dazu zählen neben den Business-Prozessen und den damit verbundenen Datenbanken auch CRM-Systeme und Webserver.

2. Die Organisation

Bei der IT-Sicherheit ist die Verantwortlichkeit organisationsübergreifend und über alle Hard- und Software-Komponenten klar zu regeln. Zudem gilt es die entsprechenden Prozesse immer wieder zu überprüfen.

Verantwortlichkeiten regeln
Die Sicherheit gehört in den Zuständigkeitsbereich der Geschäftsleitung. Die Verantwortung kann gemäss Gesetz nicht delegiert werden. Es ist allerdings möglich weitere Stellen zu bestimmen, die für die IT-Sicherheit oder Teilbereiche davon zuständig sind. Diese legen der Geschäftsleitung Bericht ab.

Die Leitungsebene muss einen Sicherheitsbeauftragten benennen, der die Informationssicherheit in der Institution fördert und den Sicherheitsprozess steuert und koordiniert. Dieser muss über angemessene zeitliche und technische Ressourcen verfügen, ausreichend qualifiziert sein und auch Gelegenheit zur Weiterbildung erhalten.

Risiken erkennen und bewerten
Eine Security Analyse identifiziert und bewertet systematisch Sicherheitsrisiken. Besonders zu beachten sind dabei die Abhängigkeiten der Geschäftsprozesse von der IT-Infrastruktur: Welche Auswirkungen haben ein teilweiser oder kompletter Systemausfall oder eine zeitweise nicht erreichbare Datenablage auf die Arbeitsabläufe eines Unternehmens? Wie gross sind die damit verbundenen finanziellen Risiken?

Im Rahmen der Analyse sind für die gesamte Informationsverarbeitung ausführliche und angemessene Sicherheitsmassnahmen festzulegen, in Sicherheitskonzepten zu dokumentieren und regelmässig zu aktualisieren.

Viren und Malware fernhalten
Eine Virenschutzsoftware allein reicht für ein KMU heute nicht mehr aus. Die Standard-Lösungen gegen Viren und Spam schützen beispielsweise nicht vor Ransomware oder Zero-Day-Angriffen:

- **Ransomware** ist für Unternehmen heute eine grosse Bedrohung. Dabei werden Geschäftsdaten verschlüsselt und erst wieder freigegeben, wenn Lösegeld bezahlt wird.
- **Zero-Day-Angriffe** nutzen Softwarelücken aus, die selbst der Hersteller noch nicht kennen, oder für die noch keine Sicherheitsupdates vorhanden sind.

Gegen solche Bedrohungsformen steht heute eine neue intelligente Sicherheitstechnik mit kognitiven Fähigkeiten zur Verfügung. Der Datenverkehr wird dabei auf Anomalien untersucht, um mögliche noch unbekannte Bedrohungen zu erkennen und abzufangen.

3. Das Personal

Ein Grossteil aller Cyberattacken kommt aus dem internen Netz. Alle Mitarbeitenden sind darum auf den angemessenen Umgang mit den Risiken zu schulen. Auch muss klar geregelt sein, an wen man sich bei Fragen oder Vorfällen richten soll.

Vertraulichkeitsklausel in Arbeitsvertrag einfügen
Geschäftsdaten sind ein schützenswertes Gut. Es empfiehlt sich, den Schutz im Rahmen einer Vertraulichkeitsklausel bereits im Arbeitsvertrag zu regeln.

Mitarbeitende auf Risiken sensibilisieren
Grosse Bedeutung hat die stetige Sensibilisierung der Mitarbeitenden auf einen risikobewussten Umgang mit der IT-Infrastruktur des Unternehmens. Dazu zählen regelmässige Sicherheitskampagnen, Schulungen, Umfragen, Merkblätter oder gar simulierte Angriffe. Zu thematisieren ist auch die private Verwendung geschäftlicher Mailadressen. So ist die Verbreitung politischer oder religiöser Ansichten mit der Firmen-Mailadresse untersagt.

Gesundes Misstrauen bewahren
Social Engineering bringt Mitarbeitende dazu, unberechtigten Dritten den Zugang zu sensiblen Daten oder ganzen IT-Systemen zu ermöglichen. Das Phishing zählt zu den bekanntesten Varianten dieser Angriffsform.

Es gilt den Mitarbeitenden den Wert von Informationen ins Gedächtnis zu rufen, sie entsprechend zu schulen und so ihr Bewusstsein zu schärfen.

Zugriff auf vertrauliche Daten regeln
Grosse Bedeutung kommt dem Umgang mit besonders vertraulichen Daten zu. Dazu zählen Kundendaten oder auch die Daten des Personalwesens. Entsprechend sind besonders geschützte Bereiche zu definieren und es gilt zu regeln, wer für welchen Zweck worauf Zugriff haben soll.

Mitarbeitende müssen mit den rechtlichen Grundlagen des Datenschutzes und den möglichen Folgen bei einem Missbrauch vertraut sein.

Gesamtlösungen aus einer Hand

Als Geschäftseinheit der GEOINFO IT AG bietet die IT-Solutions Unternehmen jeder Grösse bedarfsgerechte Informatik- und Telefonie-Dienstleistungen. Zu unseren Kunden zählen Gewerbetreibende und Ingenieurunternehmen ebenso wie Non-Profit-Organisationen und Arztpraxen.

Partner für gute und zuverlässige IT-Infrastrukturen
Besondere Bedürfnisse benötigen individuelle Lösungen. Dafür analysieren unsere Spezialisten bestehende IT-Infrastrukturen, implementieren sichere neue Lösungen und kümmern sich anschliessend um ihren reibungslosen und wirtschaftlichen Betrieb.

On Site oder in der Cloud

Unsere Kunden wählen zwischen lokalen Infrastrukturen in ihren eigenen Räumlichkeiten, dem Outsourcing in unseren Rechenzentren in Herisau und St. Gallen oder globalen Cloud Services. Auch Kombinationen sind möglich.

Schnell, sicher, persönlich
Ob vor Ort oder in der Cloud: Für eine gute und sichere IT ist die GEOINFO der richtige Ansprechpartner.

IT-Security:
Das breite Angebot der GEOINFO IT-Solutions

4. Die Hard- und Software

Alle Elemente der IT-Infrastruktur müssen immer über die aktuellsten Sicherheitsupdates verfügen. Ein Berechtigungskonzept regelt den Zugang der Mitarbeitenden auf Daten und Anwendungen.

Hard- und Software aktuell halten
Die heutigen Betriebssysteme sind in der Lage, die Anwendungen über das Internet zu aktualisieren und Fehler direkt zu beheben. Stellt ein Hersteller Schwachstellen in seiner Software fest, steht in kürzester Frist ein entsprechendes Update (Patch) zur Verfügung. Aktualisierungsintervalle sollten daher in regelmässig definierten Abständen durchgeführt werden. Bei zu grossen Zeitabständen können die Schwachstellen als Angriffspunkt dienen.

Beim Einsatz virtueller Desktops aus einer Cloud dürfen die lokalen Geräte wie Firewall, Switches oder Drucker nicht vergessen gehen. Diese wollen ebenfalls gepflegt sein.

Support- und Wartungsverträge sind regelmässig auf ihre Gültigkeit zu überprüfen, damit sich jederzeit Sicherheitsupdates beziehen und installieren lassen.

Berechtigungskonzept erstellen
Das Berechtigungskonzept hält fest, über welche Zugriffsrechte einzelne Mitarbeitende verfügen. Das schützt die technische Infrastruktur wie z.B. Systemzugänge vor fahrlässigen oder böswilligen Eingriffen (Datensicherheit) und regelt den Umgang mit vertraulichen Daten (Datenschutz).

Es ist besonders wichtig, Mitarbeitenden nur jene Rechte zu gewähren, die sie für die Ausübung ihrer Arbeit auch benötigen. Verlassen Mitarbeitende das Unternehmen, ist der Zugriff auf das interne Netz sofort zu löschen.

Logdateien sechs Monate aufbewahren
Logfiles sind wichtige Informationsquellen, um die Vorgänge auf einem System nachvollziehbar zu machen. Sie können für die Problemanalyse oder die Rekonstruktion von verloren gegangenen Daten eine enorm wichtige Rolle spielen. Viele Systeme und Anwendungen wie Domain-Controller, Firewall, E-Mail-Server oder auch eine Buchhaltungssoftware verfügen über solche Logfiles.

Logdateien sollten darum für mindestens sechs Monate aufbewahrt und im täglichen Backup-Prozess eingeschlossen werden.

5. Die Kommunikation

Die Firewall ist ein zentrales Element der IT-Security, weil sie die Kommunikation zwischen dem Netzwerk des Unternehmens und dem Internet sichert. Ebenso wichtig ist es aber, drahtlose Netzwerke zu schützen und Richtlinien für den Internetzugang zu definieren.

Netzwerkzugang über Firewall sichern
Ohne Firewall können Unbefugte unbemerkt auf den Firmenserver oder einzelne Clients zugreifen. Möglich ist dabei auch der Zugriff auf Geschäftsdaten, die dem Datenschutzgesetz unterstehen. Das kann für ein Unternehmen neben einem grossen Reputationsschaden gravierende rechtliche Folgen haben. Darum sind alle Netzwerkübergänge mit einer Firewall zu sichern, die regelmässig kontrolliert und aktualisiert wird.

Bei Remote-Zugängen ist zudem zu gewährleisten, dass der Zugriff mit einer Zwei-Faktor-Authentifizierung ausgestattet ist (One-Time Password, SMS-Token etc.). Diese Technologie ermöglicht den Einsatz von Verschlüsselungen und Zugangskontrollen in öffentlichen Netzwerken bzw. im Internet.

Drahtlose Netzwerke sichern
Bei der Verwendung drahtloser Netzwerke sind die Daten mit einem starken Algorithmus zu sichern und die Verschlüsselung mit einem dynamischen Schlüssel im WPA2-Standard zu versehen. Das Passwort sollte 12 Zeichen und mehr lang sein und aus einem wahllosen Mix aus Zeichen in Gross- und Kleinschreibung sowie Zahlen und Sonderzeichen bestehen.

Gäste-WLAN sind völlig getrennt vom internen Netzwerk z.B. über VLAN aufzubauen, um Zugriffe auszuschliessen. Drahtlose Netzwerke lassen sich ausserhalb der Bürozeiten deaktivieren.

Richtlinien für den Internetzugang definieren
Der Zugang zum Internet aus dem Firmennetzwerk darf nur im Rahmen freigegebener Verfahren, Zugriffswege und Zugangssoftware erfolgen. Alle Zugriffe sind zur Beweissicherung zu protokolieren.

Den Internetzugang zu filtern schliesst gewisse Risiken von vornherein aus. Einzelnen Mitarbeitenden kann anschliessend der Zugang auf bestimmte Seiten gezielt wieder freigegeben werden, beispielsweise Facebook für die Marketingabteilung.

6. Die Notfallvorsorge

Eine falsche Reaktion kann eine kleine Panne zum kostspieligen Totalausfall machen. Für den Notfall ist darum eine gut vorbereitete und besonnene Person in der Funktion eines Sicherheitsverantwortlichen unabdingbar.

Notfallkonzept erstellen
Das Notfallkonzept hält die Sofortmassnahmen fest, die zur Wiederherstellung des Normalbetriebs führen sollen. Dabei sind die verschiedenen Notfallszenarien und Ansprechpersonen festzulegen. Auch die für einen reduzierten Betrieb notwendigen Mittel sowie verfügbare Ausweichmöglichkeiten werden aufgeführt.

Krisenkommunikation vorbereiten
In Krisen muss auch die schnelle Kommunikation gegenüber Mitarbeitenden und Kunden sichergestellt sein: Wer kommuniziert wem wann was?

Fehler und Pannen sind nie völlig auszuschliessen. Mit der richtigen Kommunikationsstrategie lassen sich die Folgen aber zumindest eindämmen.

Ereignisse und Schwachstellen melden
Alle Mitarbeitenden müssen mit sicherheitsrelevanten Ereignissen umgehen können. Das kann das versehentliche Löschen wichtiger Daten sein, das Öffnen eines verdächtigen Mails oder der Verlust eines Laptops durch Diebstahl.

Je nach Ereignis sind andere technische Massnahmen notwendig, um das weitere Schadenmass zu begrenzen. Die zuständigen Sicherheitsverantwortlichen sind bei Vorfällen immer umgehend zu informieren.

Backup-System angemessen dimensionieren
Zwei Kennzahlen grenzen die maximalen Kosten für ein Backup-System und damit dessen notwendige Grösse ein:

- Wie viel Datenverlust (in Zeit) ist akzeptabel?
- Wie schnell müssen die Systeme wiederhergestellt sein?

Diese Kennzahlen stehen immer umgekehrt proportional zu den Kosten des Backupsystems. Zudem helfen sie beim Erarbeiten einer angemessenen Disaster-Recovery-Lösung.

Notfallmanagement überprüfen
Im angemessenen Rahmen Backups zu erstellen, ist das eine. Aber lässt sich der Datenbestand im Ernstfall dann auch schnell und sicher rekonstruieren? Um Gewissheit und damit Sicherheit zu schaffen, empfiehlt sich in regelmässigen Abständen eine Überprüfung der Effizienz des Notfallmanagements (Disaster-Recovery). Je nach Ergebnis ist an der kontinuierlichen Optimierung des implementierten Notfallmanagements zu arbeiten.

Backups auslagern
Backups sind physisch an einem anderen Ort als die Originaldaten aufzubewahren. Viele KMU setzen auf Cloud-Backups bei ihrem IT-Anbieter. Dieser überprüft die Datenkonsistenz und kann auch Restore-Tests durchführen: Erst solche Tests schaffen die Gewissheit, dass sich im Notfall die Daten auch zuverlässig wiederherstellen lassen.

Das bietet die GEOINFO

Unsere Fachkräfte helfen bei allen Fragen zur IT-Security gerne weiter. Dazu bieten wir ein ganzes Packet von Dienstleistungen. Auf Wunsch stellen wir auch bestens qualifizierte Sicherheits- und Datenschutzbeauftragte sowie Vertraulichkeitsvorlagen zur Verfügung.

Informationssicherheitsmanagement nach ISO 27001 und BSI
Wir analysieren Unternehmen mit Sicherheitsmanagement-Methoden und sichern deren Geschäftsprozesse ab.

Datenschutz-Beratung
Wir unterstützen Unternehmen bei der Umsetzung des Schweizer Datenschutzgesetzes (DSG) und der europäischen Datenschutz-Grundverordnung (DSGVO).

Risikomanagement
Wir analysieren Unternehmen mit Fokus Business Continuity auf wesentliche Risiken und halten die Resultate in einem Massnahmenkatalog fest.

IT-Security Analyse
Wir überprüfen die IT-Infrastruktur auf die korrekte Konfiguration und die Anwendung sicherer Protokolle. Aufgedeckte Schwachstellen werden beseitigt.

Workshop «Security Awareness»
Wir sensibilisieren Mitarbeitende auf Cyber-Risiken und zeigen auf, wie Gefahren erkannt und ihnen erfolgreich begegnet werden kann.

System-Monitoring
Wir bieten umfassendes Monitoring von IT-Infrastrukturen inklusive Hardware, Applikationen und Prozessen mit dem Ziel, Probleme frühzeitig zu erkennen.

Notfallplanung
Wir beraten Unternehmen bei der Notfallplanung, um Pannen schnell und effizient zu beheben und Schäden in Grenzen zu halten.

Haben Sie eine Frage oder brauchen Unterstützung?
Unter 058 580 41 41 oder it-sales@geoinfo.ch sind wir gerne für Sie da.

GEOINFO IT AG
Herisau, Oberdorfstrasse 62 | **Weinfelden,** Walkestrasse 11 | **Winterthur,** Schlosstalstrasse 49
Tel. 058 580 40 40 | it-sales@geoinfo.ch | www.geoinfo.ch/it-solutions | Mitglied der GEOINFO-Gruppe