Neun Tipps, wie Sie für mehr IT-Sicherheit im Unternehmen sorgen

Die (IT-)Sicherheit ist für viele Unternehmen ein hochbrisantes Thema – meist sehen sie sich mit immer größeren Herausforderungen konfrontiert. Ihnen wird es in Ihrem Unternehmen nicht anders gehen. Denn Cyber-Kriminelle agieren immer raffinierter und professioneller, auch bei der Wirtschaftsspionage. Nicht zuletzt wächst die Gefahr durch Viren und Trojaner stetig – und wenn man nicht aufpasst, sind E-Mail-Adressen binnen Sekunden gestohlen.

Letztlich handelt es sich hierbei um eine moderne Form der mittelalterlichen Wegelagerei. Doch diese moderne Gefahr ist sehr real. Mittelständische Unternehmen dürfen es sich heute nicht mehr erlauben, all die drängenden Sicherheitsthemen aus den Augen zu verlieren: Daten- und Know-how-Verlust, Informationsdiebstahl, Arbeitsausfälle, die daraus resultierenden explodierenden Kosten für EDV bis hin zur Strafverfolgung, wenn es zu Schäden kommt. Gravierende Sicherheitsmängel haben immer auch hohe Umsatzeinbußen zur Folge.

Heute ist es wichtiger denn je, eine stabile, funktionale und sichere IT-Infrastruktur bereitzustellen – was wiederum Aufwände verursacht, die durch die eigenen Mitarbeiter kaum zu stemmen sind. Damit Sie sich in Ihrem Unternehmen gegen diese Angriffe und Ausfälle wappnen können, hat die abass GmbH eine Checkliste mit neun zentralen Tipps zusammengestellt. Wenn Sie alle Punkte bereits abhaken können: Glückwunsch! Ansonsten können Sie sehr gerne auf unser Fachwissen und unsere Unterstützung zurückgreifen – sprechen Sie uns einfach an.

Tipp 1:
Den Zugang zum Gebäude sichern

Habe ich den Zugang zu meinem Gebäude bereits durch eine Pforte oder andere Sicherheitstechniken beschränkt?

✓

Falls ja, sollten Sie nichtsdestotrotz immer wachsam sein und darauf achten, wenn Ihnen im Flur eine Person begegnet, die Sie nicht kennen. Diese Person sollten Sie in jedem Fall ansprechen und nach ihrer Aufenthaltsberechtigung fragen.

✗

Falls nein, sollten Sie einen Dienstleister zurate ziehen.

Die abass GmbH kann Sie entscheidend unterstützen:

- ✓ Durchführung von Sicherheitsworkshops für alle Mitarbeiter, um sie für die Gefahren zu sensibilisieren.
- ✓ Durchführung einer Sicherheitsprüfung im Unternehmen: Im Zuge eines Sicherheits-Audits wird abass Ihnen unangekündigt und inkognito mit verdeckten Ermittlern einen Besuch abstatten und testen, wie weit Unbefugte in Ihr Unternehmen vordringen können, ohne bemerkt zu werden. Auf Basis des Audit-Ergebnisses können wir anschließend gemeinsam mit Ihnen ein Sicherheitskonzept erarbeiten.

Mögliche Lösungsoptionen:

- ✓ Einrichten einer Pforte, bei der ein Pförtner jede Person, die Zutritt zum Unternehmen wünscht, zuerst anmeldet. Der Besucher wird anschließend von einem Mitarbeiter abgeholt und in das Büro begleitet – oder direkt beim Verlassen des Aufzugs in Empfang genommen.
- ✓ Einrichten eines Sicherheitssystems, etwa durch Kameraequipment, auf das Mitarbeiter im Unternehmen permanent Zugriff haben und mit dem sie überblicken können, welche Personen das Gebäude betreten.

Tipp 2:
Sicheres Arbeiten mit dem Computer

Haben Sie Ihre Mitarbeiter bereits im Umgang mit dem sicheren Arbeiten am Computer geschult? Etwa hinsichtlich Themen wie:

- Die Bildschirmsperre zu aktivieren, wenn ein Mitarbeiter den Platz verlässt
- Passwörter regelmäßig zu ändern (alle 90 Tage mindestens einmal)
- Nicht überall das gleiche Passwort zu verwenden

✓

Falls ja, sollten Sie dennoch das Wissen Ihrer Mitarbeiter über diese wichtigen Sicherheitsthemen immer wieder auffrischen.

✗

Falls nein, sollten Sie einen Dienstleister zurate ziehen.

Die abass GmbH kann Sie entscheidend unterstützen:

- ✓ Durchführung von Workshops für die Mitarbeiter.
- ✓ Einrichten von Erinnerungen, die die Mitarbeiter beispielsweise darauf hinweisen, ihr Passwort zu ändern. Oder auch eine Einrichtung einer automatischen Bildschirmsperrung, bereits nach wenigen Minuten ohne Tastatureingabe.

Tipp 3:
Umsichtiges Surfverhalten

Haben Sie Ihre Mitarbeiter bereits im Umgang mit Ihrem Surfverhalten am Arbeitsplatz geschult? Darunter fallen Aspekte wie:

- Dass die Mitarbeiter aufmerksam sein müssen, wenn sie im Internet etwas bestellen; Stichwort: vertrauenswürdige Websites
- Dass sie generell umsichtig sein sollten, auf welchen Websites sie sich im Internet bewegen
- Dass sie vorsichtig bei der Eingabe von Sicherheitscodes (PIN oder TAN) sein müssen
- Dass sie Apps nur über vertrauenswürdige Quellen beziehen
- Dass nichts im Internet kostenlos ist, auch wenn es auf den ersten Blick so scheint. Man bezahlt immer – und sei es mit den eigenen Daten

✓

Falls ja, sollten Sie Ihre Mitarbeiter nichtsdestotrotz immer auf dem Laufenden halten und das Wissen regelmäßig durch Schulungen auffrischen.

✗

Falls nein, sollten Sie einen Dienstleister zurate ziehen.

Die abass GmbH kann Sie entscheidend unterstützen:

- ✓ Durchführung von Workshops für die Mitarbeiter.
- ✓ Einrichten von Filtersoftware, die den Zugang zu sicherheitskritischen Websites unterbindet.

Tipp 4:
Clean Desk-Policy

Haben Sie Ihre Mitarbeiter bereits im Umgang mit dem Thema „Sauberer Arbeitsplatz“ vertraut gemacht? Das betrifft:

• Das Liegenlassen von sensiblen Dokumenten wie Kundenunterlagen, Akten, Plänen o.ä. am Arbeitsplatz, wenn dieser unbeaufsichtigt ist, genauso wie das Liegenlassen von Handys.
• Das Aufschreiben von Passwörtern, die dann offen am Arbeitsplatz abgelegt werden.
• Notizen in den Papierkorb zu werfen, anstatt sie ordnungsgemäß zu vernichten.
Die EU-Datenschutzgrundverordnung (DSGVO) ahndet es sogar mit hohen Strafen, wenn ein Unternehmen seine Clean Desk-Policy vernachlässigt.

✓

Falls ja, sollten Sie nichtsdestotrotz das Wissen Ihrer Mitarbeiter hinsichtlich dieser wichtigen Sicherheitsthemen immer wieder auffrischen – das betrifft insbesondere die neuen Richtlinien, die seit Inkrafttreten der DSGVO wirksam sind. Viele Unternehmen haben es bisher versäumt, dieses Wissen aufzufrischen.

✗

Falls nein, sollten Sie auch für diesen Bereich einen Dienstleister zurate ziehen.

Die abass GmbH kann Sie entscheidend unterstützen:

- ✓ Durchführung von Workshops für die Mitarbeiter
- ✓ Einrichten einer DSGVO-konformen Clean Desk-Policy im Unternehmen. Gemeinsam mit Ihnen werden wir ein Konzept für eine solche Richtlinie erarbeiten und durch Schulungen an die Mitarbeiter weitergeben.

Mögliche Lösungsoptionen:

- ✓ Der Arbeitsplatz der Zukunft ist digital. Darum können Sie viele dieser Sicherheitsrisiken beheben, indem Sie Prozesse digitalisieren. Sei es, dass Sie Ihren Mitarbeitern einen Passwortmanager auf dem PC bereitstellen oder dass Sie Systeme zur Verfügung stellen, in denen die Mitarbeiter relevante Dokumente in digitaler Form einsehen, bearbeiten und ablegen können.

Tipp 5:
Sichere Telefonie

Haben Sie Ihre Mitarbeiter bereits im Umgang mit der Herausgabe von sensiblen Daten via Telefon geschult? Das betrifft folgende Themen:

- Die Herausgabe von unternehmenssensiblen Daten
- Die Herausgabe von personenbezogenen Mitarbeiterdaten, etwa „Nein, Kollege XY ist heute nicht im Haus. Er ist krank."
- Den (schnellen) Kaufabschluss über das Telefon

✓

Falls ja, sollten Sie nichtsdestotrotz das Wissen Ihrer Mitarbeiter hinsichtlich dieser wichtigen Sicherheitsthemen immer wieder auffrischen – seit Inkrafttreten der DSGVO betrifft dies insbesondere auch den Umgang mit personenbezogenen Daten. Viele Unternehmen haben es bisher versäumt, ihre Mitarbeiter im Umgang mit diesem sensiblen Thema zu schulen.

✗

Falls nein, sollten Sie auch für diesen Bereich einen Dienstleister zurate ziehen. Die Telefonie ist sicherlich einer der wenigen Bereiche, der sich nicht digital absichern lässt, weil zumeist Menschen und keine Maschinen ans Telefon gehen. Es gibt auch Videos, die verdeutlichen, wie schnell es gelingen kann, durch das Vorspielen falscher Tatsachen (Die Frau eines Mitarbeiters ruft an, im Hintergrund schreiendes Kind, sie braucht unbedingt den Kontakt zu ihrem angeblichen Ehemann) an sensible Informationen wie etwa die Handynummer eines Mitarbeiters zu gelangen. Gerade deshalb ist es ratsam, sich an einen kompetenten Dienstleister zu wenden.

Die abass GmbH kann Sie entscheidend unterstützen:

- ✓ Durchführung von Workshops für die Mitarbeiter, in denen folgende Fragen beantwortet werden
  - Welche Daten darf ich am Telefon preisgeben?
  - Wie überprüfe ich die Telefonnummern eingehender Anrufe?
  - Warum sollte ich besser keine schnellen Käufe über das Telefon tätigen?

Tipp 6:
Datensicherung

Haben Sie bereits ein mehrstufiges Datensicherheitsverfahren in Ihrem Unternehmen etabliert? Wenn Sie sich im Unklaren darüber sind, wie hoch Sie die Relevanz der Datensicherheit bewerten sollen, dann stellen Sie sich am besten die Frage, wie lange Ihr Unternehmen ohne wichtige Daten überleben kann. Je kürzer dieser Zeitraum ist, desto umfangreicher sollte die Sicherung dieser Daten ausfallen.

✓

Falls ja, sollten Sie trotzdem überlegen, ob es nicht vielleicht sinnvoll ist, das Vorgehen hinsichtlich der Datensicherung noch einmal kritisch zu hinterfragen. Eventuell gibt es inzwischen neue Techniken oder Methoden, die für Ihre Bedürfnisse besser geeignet sind.

✗

Falls nein, sollten Sie einen Dienstleister zurate ziehen. Denn Datensicherheit ist ein äußerst wichtiges Thema, und insbesondere kleinere und mittelständische Unternehmen verfügen häufig nicht über die Systeme oder Kapazitäten, die notwendig sind, um selbst ein regelmäßiges Datenbackup durchzuführen.

Die abass GmbH kann Sie entscheidend unterstützen:

- ✓ Systemanalyse, um zunächst zu klären, welches Datensicherungskonzept in Ihrem Fall das richtige ist – denn das Konzept muss zu Ihrem Unternehmen passen. Die abass GmbH bietet Ihnen nicht nur die dafür notwendige Beratung, sondern entwickelt individuelle, auf Sie zugeschnittene Konzepte und Lösungen.

- ✓ Einrichten eines mehrstufigen Datensicherheitsverfahrens (kurzfristig – langfristig).

Mögliche Lösungsoptionen:

- ✓ Einrichten einer Cloud-Lösung. Diese eignet sich besonders gut für Unternehmen, die länderübergreifend zusammenarbeiten und beispielsweise von verschiedenen Standorten aus auf dieselben Daten zugreifen müssen. Jedoch ist eine sehr gute Internetbandbreite erforderlich, um Daten bedarfsgerecht up- und downloaden zu können.

- ✓ Entwicklung eines Datensicherungskonzeptes mit jährlicher Überprüfung durch Zurückspielen der Datensicherung.

Tipp 7:
Serverraum vor unbefugtem Zutritt schützen

Haben Sie Ihren Serverraum oder Ihren Serverschrank vor unbefugtem Zugriff geschützt? Viele Unternehmen unterschätzen diese Problematik. Tatsächlich ist es aber schon vorgekommen, dass der Serverraum nicht abgeschlossen war und die Reinigungskraft, die für ihre Reinigung eine Steckdose brauchte, im Serverraum einfach irgendeinen Stecker gezogen hat – mit den zu erwartenden höchst unangenehmen Folgen.

✓

Falls ja, sollten Sie dafür Sorge tragen, dass der Zutritt nur den zuständigen Mitarbeitern möglich ist. Muss der Raum etwa gereinigt werden, dann sollte dies immer unter Aufsicht geschehen – und die Putzkraft ist vom Unternehmen entsprechend zu schulen.

✗

Falls nein, sollten Sie dagegen unbedingt vorgehen. Denn ein unbefugter Zugriff auf den Server kann katastrophale Schäden zur Folge haben. Ziehen Sie also einen kompetenten Dienstleister zurate.

Die abass GmbH kann Sie entscheidend unterstützen:

- ✓ Durchführung von Workshops für die Mitarbeiter.
- ✓ Einrichten von Erinnerungen, die die Mitarbeiter beispielsweise darauf hinweisen, ihr Passwort zu ändern. Oder auch eine Einrichtung einer automatischen Bildschirmsperrung, bereits nach wenigen Minuten ohne Tastatureingabe.

Tipp 8:
Mitarbeiterausfall wegen Urlaub

Haben Sie genügend IT-Mitarbeiter, die den Aus- bzw. Wegfall eines Mitarbeiters während seines Urlaubs oder wegen einer anderen Abwesenheit kompensieren können?

✓

Falls ja, sollten Sie dafür Sorge tragen, dass die Übergabe von einem Mitarbeiter zum anderen reibungslos über die Bühne geht, damit für eine konsistente IT-Sicherheit gesorgt ist.

✗

Falls nein, sollten Sie sich gegen solche Fälle absichern und die Ressourcen eines Dienstleisters in Anspruch nehmen.

Die abass GmbH kann Sie entscheidend unterstützen:

- ✓ Entweder in Form von personellen Ressourcen, die sich direkt vor Ort um die Belange Ihrer IT kümmern und die Abwesenheit Ihres Mitarbeiters perfekt kompensieren.
- ✓ Oder indem wir entsprechende Infrastrukturen bereitstellen, etwa um Sie via Remotezugriff in allen IT-Belangen unterstützen zu können.

Tipp 9:
Geregeltes Patch-Management

Haben Sie einen oder mehrere Mitarbeiter, die sich darum kümmern, dass auf allen Systemen in Ihrem Unternehmen jede Software auf einem aktuellen Update-Stand ist?

✓

Falls ja, sollten Sie unbedingt darauf achten, dass wirklich alle Updates ausgeführt wurden. Nichts birgt ein höheres Risiko als Systeme, die für Schadsoftware anfällig werden, weil keine regelmäßigen (Sicherheits-)Updates erfolgt sind.

✗

Falls nein, sollten Sie sich gegen solche Fälle absichern und einen Dienstleister zurate ziehen.

Die abass GmbH kann Sie entscheidend unterstützen:

- ✓ Beratung, welches Konzept des Patch Managements für Sie das beste ist.
- ✓ Bedarfsgerechte Bereitstellung, Installation und Betreuung unterschiedlicher Patch-Management-Systeme.
  - Beispiel-System: ManageEngine Patch Manager Plus
  - Beispiel-System: baramundi Patch-Management-System

Fazit: Die Zeit, zu handeln, ist jetzt

Haben Sie bei sich im Unternehmen noch Lücken identifiziert, nachdem Sie unsere Checkliste zur IT-Sicherheit durchgegangen sind? Manches werden Sie vielleicht selbst beheben können, aber für viele Maßnahmen ist es sicherlich sinnvoller, wenn Sie sich externe Hilfe holen. Die abass GmbH unterstützt Sie gerne dabei, ein ausführliches IT-Sicherheitskonzept für Ihren Bedarf zu erarbeiten und in Ihrem Unternehmen umzusetzen. Wir freuen uns darauf, Sie in all Ihren IT-Belangen zu unterstützen, auch in Sicherheitsfragen.

Bitte kontaktieren Sie uns einfach!