suissetec

Schweizerisch-Liechtensteinischer Gebäudetechnikverband
Association suisse et liechtensteinoise de la technique du bâtiment
Associazione svizzera e del Liechtenstein della tecnica della costruzione
Associaziun svizra e liechtensteinaisa da la tecnica da construcziun

Januar 2018

Merkblatt

IT-Sicherheit für KMU

**Mehr Informationssicherheit für Klein- und Mittelbetriebe (KMU):
Das 10-Punkte-Programm des Vereins ISSS schafft mehr Schutz**

Einleitung

Die Schweiz zählt im weltweiten Vergleich zu den Spitzenanwendern von Informations- und Kommunikationstechnologien. Niemand gibt weltweit mehr Geld pro Kopf für Informationstechnologie aus als Herr und Frau Schweizer. Es ist klar, ohne IT läuft nichts!
Dieses Merkblatt richtet sich an KMU und soll diesen dabei helfen, die IT-Sicherheit im Unternehmensnetzwerk zu erhöhen. Das 10-Punkte-Programm ist einfach gehalten und Sie können die Massnahmen realisieren, ohne dass für Sie grosse Kosten entstehen. Wo das spezifische Fachwissen in einem kleinen oder mittleren Betrieb nicht verfügbar ist, lassen Sie sich von einem Experten unterstützen.
Wir weisen darauf hin, dass technische Massnahmen alleine nicht genügen, um die IT-Sicherheit in einem Unternehmensnetzwerk zu gewährleisten. Zusätzlich sind immer auch organisatorische Massnahmen notwendig. Gerade bei kosten- und/oder ressourcenintensiven Massnahmen muss jede Firma, konkret die Geschäftsleitung, eine Abwägung treffen zwischen den Kosten dieser Massnahme und den Risiken, die bei einer Nichtumsetzung der Massnahme entstehen. Die Geschäftsleitung muss deshalb entscheiden, entsprechende Risiken zu tragen oder Ressourcen bereitzustellen, um sie zu minimieren.

Das 10-Punkte-Programm im Überblick:

Zehn Massnahmen für einen wirkungsvollen Grundschutz

1. Erstellen Sie ein Pflichtenheft für IT-Verantwortliche!
2. Sichern Sie Ihre Daten regelmässig mit Backups!
3. Halten Sie Ihr Antivirus-Programm aktuell!
4. Schützen Sie Ihren Internetzugang mit einer Firewall!
5. Aktualisieren Sie Ihre Software regelmässig!
6. Verwenden Sie starke Passwörter!
7. Schützen Sie Ihre mobilen Geräte!
8. Machen Sie Ihre IT-Benutzerrichtlinien bekannt!
9. Schützen Sie die Umgebung Ihrer IT-Infrastruktur!
10. Ordnen Sie Ihre Dokumente und Datenträger!

1

Erstellen Sie ein Pflichtenheft für IT-Verantwortliche!

Grundsätze

IT-Sicherheit beruht zu je einem Drittel auf technischen, organisatorischen und menschlichen Faktoren!
Neben technischen Sicherheitslösungen und motivierten Mitarbeitenden muss auch die Geschäftsleitung ihren Beitrag zu einem wirkungsvollen Grundschutz leisten.

Erläuterungen:

- Jedes Unternehmen braucht einen EDV- bzw. IT-Verantwortlichen mit Stellvertreter. Das nötige Wissen dazu kann in entsprechenden Kursen erworben werden. Oft arbeiten kleine Unternehmen auch mit externen Spezialisten zusammen. Die Kosten hierfür sind wesentlich tiefer als die Folgen eines Datenverlustes oder eines Verstosses gegen das Datenschutzgesetz.
- Die Geschäftsleitung delegiert Sicherheitsaufgaben an den IT-Verantwortlichen schriftlich und hält diese in einem Pflichtenheft fest (siehe rechts).

Tipps & Tricks:

Richtlinien für IT-Verantwortliche

- Sichern Sie die Daten auf Servern, Arbeitsstationen, Notebooks, Laptops und anderen mobilen Geräten regelmässig (siehe Punkt 2).
- Halten Sie Betriebssysteme, Antivirus-Programme, Firewalls und sonstige Software aktuell (siehe Punkte 3, 4 und 5).
- Ändern Sie werkseitige Passworteinstellungen bei Geräten, Betriebssystemen und Anwendungsprogrammen sofort.
- Führen Sie eine Liste mit allen im Unternehmen vorhandenen Computern, mit den installierten Programmen sowie den ausgeführten Software-Aktualisierungen (siehe Punkt 5).
- Die Geschäftsleitung kontrolliert, ob der IT-Verantwortliche seine Aufgaben korrekt wahrnimmt.
- Alle Mitarbeitenden, die an einem Computer arbeiten, erhalten Benutzerrichtlinien. Diese beschreiben, welche Aktionen auf dem Computer erlaubt und welche untersagt sind (siehe Punkt 8).
- Bestimmen Sie einen Ansprechpartner für alle Sicherheitsfragen, z. B. bei einem Verlust von Notebooks oder bei einem Virenbefall usw.
- Legen Sie die Zugriffsrechte fest: Welche Programme dürfen Mitarbeitende ausführen? Auf welche Daten haben Mitarbeitende Zugriff?
- Führen Sie eine Liste mit allen Personen, welche von aussen auf das Firmennetzwerk zugreifen, eventuell mit genauer Dauer der Berechtigung. Stellen Sie sicher, dass auch deren Schutzprogramme aktuell sind.
- Stellen Sie sicher, dass Datenschutz-Bestimmungen eingehalten werden, z. B. durch aktuelle Schutzprogramme und starke Passwörter (siehe Punkte 3, 4, 6).
- Kontrollieren Sie regelmässig, ob die Benutzerrichtlinien eingehalten werden.

2

Sichern Sie Ihre Daten regelmässig mit Backups!

Grundsätze

Datenverluste entstehen auf verschiedene Arten: Daten werden versehentlich überschrieben, Informationen auf einer Harddisk werden durch einen Defekt unleserlich oder ein Brand beziehungsweise ein Wasserschaden zerstört Ihre Daten. Solche Verluste können Sie mit regelmässigen Datensicherungen (Backups) vermeiden.

Erläuterungen:

- Grundsätzlich sind alle Daten mit geschäftsrelevantem Inhalt zu sichern. Softwarekonfigurationen sollten ebenfalls gesichert werden.
- Die Häufigkeit der Datensicherung richtet sich nach der Tätigkeit und Grösse Ihres Unternehmens. Mindestens einmal pro Woche sollte jeder kleine oder mittlere Betrieb seine Daten sichern.
- Ein Betrieb mit einem täglichen Backup sorgt für die gesetzeskonforme Archivierung Ihrer Daten gemäss Obligationenrecht und der «Verordnung über die Führung und Aufbewahrung der Geschäftsbücher» (GeBüV) (siehe rechts).

Tipps & Tricks:

Richtlinien zum Thema Backup

- Erstellen Sie von Montag bis Donnerstag je ein Tages-Backup auf einem eigenen Speichermedium. Die Tages-Backups werden jeweils am selben Wochentag in der folgenden Woche überschrieben. Bewahren Sie die Tageskopien ausserhalb des Serverraums auf.
- Erstellen Sie jeden Freitag ein Wochen-Backup auf einem separaten Speichermedium und bewahren Sie dieses ausserhalb des Betriebs auf. Das Wochen-Backup wird nach einem Monat wieder überschrieben.
- Regeln Sie schriftlich, wer für Datensicherungen zuständig ist, und führen Sie eine Kontrollliste über die erfolgreiche Sicherung der Daten.
- Sichern Sie die Daten immer auf mobilen Medien (Bandlaufwerk, auswechselbarer Datenträger).
- Es lohnt sich, von wichtigen Daten, die nur in Papierform vorliegen (z. B. Verträge, Urkunden), Kopien anzufertigen und diese ebenfalls ausser Haus aufzubewahren.
- Beachten Sie, dass die Bilanz, die Erfolgsrechnung, die Geschäftsbücher, die Inventare, die Buchungsbelege und die Geschäftskorrespondenz während 10 Jahren aufbewahrt werden müssen.
- Erstellen Sie am Monatsende das Monats-Backup. Das Monats-Backup wird nicht mehr überschrieben und ausserhalb des Betriebs aufbewahrt.
- Erstellen Sie Ende Jahr das Jahres-Backup. Das Jahres-Backup wird nicht mehr überschrieben und ebenfalls ausserhalb des Betriebs aufbewahrt.
- Überprüfen Sie periodisch, ob sich die Daten von den Sicherungsmedien zurückspielen lassen. Jede Sicherung ist nutzlos, wenn die Daten nicht korrekt auf das Backup-Medium übertragen wurden.

3

Halten Sie Ihr Antivirus-Programm aktuell!

Grundsätze

Schädliche Programme wie zum Beispiel Viren und Würmer können Ihre IT-Infrastruktur lahmlegen und damit die wirtschaftliche Existenz Ihres Unternehmens gefährden.

Erläuterungen:

- Computerviren können Daten und Programme verändern, manipulieren oder sogar vollständig zerstören. Bösartige Computerprogramme werden via E-Mail-Anhänge (Attachments) und Instant Messengers usw. übertragen. Im Internet sind Viren oft als nützliche oder unterhaltende Gratisprogramme getarnt und werden durch einen einfachen Mausklick aktiviert.
- Unzureichend geschützte Computersysteme werden häufig zur Verbreitung von Viren und für gezielte Attacken gegen ein drittes Unternehmen missbraucht. Wer als Geschäftsleiterin oder Geschäftsleiter ungenügende Vorkehrungen zum Schutz der firmeninternen Computersysteme trifft, handelt fahrlässig und muss allenfalls mit Strafverfolgung rechnen.

Tipps & Tricks:

Richtlinien zum Thema Virenschutz

- Installieren Sie ein Antivirus-Programm auf sämtlichen Servern, Arbeitsstationen (Clients) sowie Ihren Notebooks und aktualisieren Sie den Schutz regelmässig, also mindestens täglich.
- Untersagen Sie ausdrücklich das Ausschalten oder zeitweise Deaktivieren des Antivirus-Programms.
- Fordern Sie die Mitarbeitenden auf, Warnmeldungen über Viren unverzüglich dem IT-Verantwortlichen zu melden.
- Schutz vor bekannten Viren und Würmern bietet ein Antivirus-Programm. Es identifiziert Eindringlinge und macht sie unschädlich. Solche Programme können in Computerläden gekauft oder kostenlos aus dem Internet heruntergeladen werden.
- Da Hacker laufend neue Viren programmieren, muss das Antivirus-Programm immer wieder aktualisiert werden. Je nach verwendetem Produkt sucht das Programm auf der Homepage des Herstellers selbstständig nach solchen Aktualisierungen. Informieren Sie sich bei Ihrem Händler, ob dies bei Ihrem Programm der Fall ist. Die Aktualisierung sollte auf jeden Fall täglich durchgeführt werden.
- Führen Sie mindestens einmal wöchentlich einen vollständigen «Virus-Scan» der Festplatten durch. Damit werden bisher unerkannte Viren entdeckt und eliminiert.
- Untersagen Sie eigene Tests mit Viren ausdrücklich.
- Aktualisieren Sie bei grösseren Netzwerken Antivirus-Programme zentral und automatisch.

4

Schützen Sie Ihren Internetzugang mit einer Firewall!

Grundsätze

Gibt es in Ihrem Betrieb Brandschutztüren? Ja? Dann achten Sie bestimmt darauf, dass diese Türen auch stets geschlossen werden.
In der Welt des Internets und des elektronischen Datenaustauschs erfüllt die Firewall diese Sicherheitsaufgabe.

Erläuterungen:

- Ohne eine Firewall können Unbefugte auf Ihren Computersystemen Schaden anrichten. Sie können darauf unbemerkt Befehle ausführen oder Ihre Rechner zu illegalen Attacken gegen Dritte missbrauchen. Zudem gelangen sie an Geschäftsdaten, die eventuell dem Datenschutzgesetz unterstehen.
- Für grössere Firmennetzwerke ist eine eigenständige Firewall (spezielles Gerät), für einzelne PCs und mobile Geräte (Notebooks) eine integrierte Firewall (auf dem System selbst) zu empfehlen.
- Im Handel sind Produkte erhältlich, die gleichzeitig eine Firewall und einen Virenschutz bieten. Gerade für kleinere Betriebe sind kombinierte Produkte sehr zu empfehlen.

Tipps & Tricks:

Richtlinien zum Thema Firewall

- Installieren Sie eine Firewall und aktualisieren Sie diese regelmässig.
- Wickeln Sie den gesamten Internetverkehr über die Firewall ab. Erlauben Sie keine anderen Zugänge zum Internet (z. B. via Modem).
- Setzen Sie im Unternehmen keine privaten Laptops und Wireless-LAN-Geräte ohne schriftliche Einwilligung des IT-Verantwortlichen ein.
- Manche Betriebssysteme haben eine eigene Firewall eingebaut. Nutzen Sie auf jeden Fall auch diese Möglichkeit und aktivieren Sie diese Firewalls.
- Wenn Sie in Ihrem Betrieb Wireless LAN für Ihre Computer einsetzen, sorgen Sie dafür, dass es richtig und sicher funktioniert. Falsch genutzte Wireless-LAN-Geräte machen den gesamten Firewall-Schutz zunichte.
- Sämtliche Netzwerkübergänge müssen mit einer Firewall gesichert werden. Alle Verbindungen zwischen Lieferanten, Kunden, Outsourcern und Mitarbeitenden (auch mit Remote Access) und Ihrem Netzwerk müssen durch eine Firewall kontrolliert werden.
- Schützen Sie die Konfiguration Ihrer Firewall mit einem starken Passwort.
- Sichern Sie die Konfiguration der zentralen Firewall regelmässig.

5

Aktualisieren Sie Ihre Software regelmässig!

Grundsätze

Kontrollieren Sie bei Ihrem Auto regelmässig Ölstand und Reifendruck? Hoffentlich.
So wie Sie Ihr Auto regelmässig warten, müssen auch Computerprogramme in einem Unternehmen gepflegt und auf den neuesten Stand gebracht werden.

Erläuterungen:

- Heutige Software beinhaltet oft Millionen von Codezeilen. Dabei schleichen sich trotz Kontrollen Fehler ein. Für den Hersteller ist es nahezu unmöglich, Anwendungen in jeder denkbaren Umgebung und möglichen Konfiguration zu testen. Die Hersteller bieten regelmässig sogenannte «Patches», also «Software-Flicken», an. Diese beheben die bekannten Fehler.
- Wenn Sie Ihre Software nicht oder nur selten aktualisieren, können Angreifer bekannte Fehler ausnützen, um Daten zu manipulieren oder um Ihre Infrastruktur für bösartige Zwecke zu missbrauchen.
- Häufig sind Betriebssysteme und Anwendungen in der Lage, sich selbst über das Internet zu aktualisieren. Die Webseiten der Software-Hersteller und das Handbuch helfen hier weiter.

Tipps & Tricks:

Richtlinien zum Thema Patches

- Installieren Sie die neuesten «Patches» für Betriebssysteme und Anwendungsprogramme.
- Installieren Sie verfügbare «Sicherheits-Updates» so schnell wie möglich.
- Installieren Sie nur Aktualisierungen für die Versionen einer Software, die Sie verwenden.
- Minimieren Sie Ihre «Angriffsfläche», indem Sie nur Software installieren, die Sie tatsächlich benötigen, und unnötige Dienste, Netzwerkfreigaben und Protokolle deaktivieren. Was nicht vorhanden ist, kann nicht missbraucht werden und muss nicht gepflegt werden!
- Wenn Sie selber Schwachstellen entdecken oder sich die Software eigenartig verhält, informieren Sie Ihren Software-Hersteller.
- Installieren Sie «Patches» auf sämtlichen Computern, d. h. auch auf Notebooks und Geräten von externen Mitarbeitenden!
- Führen Sie eine Liste darüber, welche «Updates» wo installiert sind.

Hier finden Sie die neuesten «Updates» für die Microsoft-Produkte: www.windowsupdate.com

6

Verwenden Sie starke Passwörter

Grundsätze

Wer den Benutzernamen und das Passwort eines Anwenders kennt, kann sich bei einem System anmelden und übernimmt damit die (Computer-)Identität des entsprechenden Anwenders mit allen Zugriffsberechtigungen!
Durch Passwortdiebstahl können somit Unbefugte ohne grossen Aufwand an vertrauliche Geschäftsinformationen gelangen. Verhindern Sie also, dass in Ihrem Betrieb ein Identitätsdiebstahl möglich ist.

Erläuterungen:

- Werkseitige Passworteinstellungen bei Geräten, Betriebssystemen und Anwendungsprogrammen müssen vom IT-Verantwortlichen sofort geändert werden (siehe Punkt 1).
- Halten Sie Ihre Mitarbeitenden dazu an, nur starke Passwörter einzusetzen, die regelmässig geändert werden. Machen Sie allen bewusst, dass sie für Handlungen verantwortlich sind, die unter ihrem Benutzernamen ausgeführt werden.
- Starke Passwörter sind mindestens 9 Zeichen lang, enthalten Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen.

Tipps & Tricks:

Richtlinien zum Thema Passwörter

- Verwenden Sie keine Passwörter, die in Wörterbüchern zu finden sind.
- Verwenden Sie keine Passwörter, die Namen, AHV- und Passnummern oder Geburtsdaten aus dem Familienumfeld enthalten.
- Prüfen Sie die Qualität eines Passwortes mit einem Passwort-Checker.
- So können Sie starke Passwörter konstruieren:
  Beispiel 1: Aus dem einfachen Wort «Sommer» leiten Sie das starke Passwort «So$Mmer04» ab, indem Sie an der 3. Stelle «$» einfügen, gross weiterfahren und am Ende noch die Ziffer «04» für den Monat April ergänzen.
  Beispiel 2: Aus dem Satz «Letzten Sommer waren wir zu viert in Paris!» leiten Sie das starke Passwort «LSwwz4iP!» ab, indem Sie Anfangsbuchstaben und Ziffern aneinanderreihen. Einen vernünftigen Satz kann man sich besser merken als ein kryptisches Passwort!
- Schreiben Sie Passwörter niemals auf, ohne die Notiz sicher, z. B. im Tresor, zu verwahren. Viele Passwörter findet man aufgeschrieben im Umkreis von einem Meter beim Computer.
- Geben Sie Ihr Passwort niemals an Dritte weiter. Stellvertretungen funktionieren auch ohne Kenntnis des Passworts. Falls Sie feststellen, dass Dritte Ihr Passwort kennen, ändern Sie es umgehend.

Hier können Sie die Qualität Ihres Passwortes überprüfen lassen: https://passwortcheck.datenschutz.ch/

7

Schützen Sie Ihre mobilen Geräte!

Grundsätze

Mobiltelefone, Handheld-Computer und Notebooks mit Wireless LAN sind ausgesprochen praktisch und vielseitig. Falsch eingesetzt, stellen diese Geräte aber ein Sicherheitsrisiko dar. Wer aus geschäftlichen Gründen gezwungen ist, sensible Daten auf mobilen Geräten zu speichern, muss spezielle Vorkehrungen treffen.

Erläuterungen:

- Sämtliche mobilen Geräte müssen mit einem starken Passwort geschützt werden (siehe Punkt 6). Beim Verlust des Geräts oder im Fall eines Diebstahls haben Unbefugte sonst ein leichtes Spiel, an Ihre Geschäftsdaten zu gelangen.
- Auf mobilen Geräten sollten nur diejenigen Daten enthalten sein, die tatsächlich benötigt werden. Sichern Sie diese regelmässig (siehe Punkt 2).
- Heikle Geschäftsdaten auf Notebooks müssen verschlüsselt gespeichert werden, damit sie bei Verlust oder Diebstahl nicht in die Hände Unbefugter geraten. Gute Verschlüsselungsprogramme sind im Handel erhältlich und können auch aus dem Internet heruntergeladen werden (siehe rechts).

Tipps & Tricks:

Richtlinien zum Thema Wireless LAN

- Ändern Sie den vom Hersteller vorgegebenen Namen für Ihr Wireless LAN (Service Set Identifier – SSID). Die neue Identifikation darf keinesfalls Ihren Firmennamen enthalten.
- Deaktivieren Sie die SSID-Ausstrahlung, damit Ihr Access Point für Dritte nicht sichtbar ist.
- Aktivieren Sie die Verschlüsselung der kabellosen Datenübermittlung (WPA2, Wi-Fi Protected Access 2). Ändern Sie das Standard-Passwort Ihres Access Points.
- Auch mobile Geräte müssen regelmässig auf Viren geprüft werden, weil sie z. B. via E-Mail-Funktionen mit Ihren übrigen Computern synchronisiert werden.
- Durch falsch konfigurierte Wireless-LAN-Geräte können Hacker innerhalb weniger Minuten aus Distanzen von über einem Kilometer in Ihr Firmennetzwerk eindringen! Die Nutzung von externen und öffentlichen Access Points (Hotspots) muss speziell geregelt werden.
- Aktivieren Sie Bluetooth bei Ihren Geräten (Handy, Notebooks, Handheld-Computer) nur bei Bedarf und nicht erkennbar. Ihr Gerät reagiert sonst ohne Ihr Wissen auf Anfragen fremder Geräte (im Umkreis von bis zu 100 Metern).
- Setzen Sie den MAC-Adressfilter ein, damit nur bekannte Geräte mit dem Access Point kommunizieren können.
- Übermitteln Sie hoch vertrauliche Daten nur über Verbindungen, welche zusätzlich mit einem Virtual Private Network (VPN) geschützt sind.
- Zur Verschlüsselung können Sie das Produkt Pretty Good Privacy (PGP) verwenden. Sie finden PGP für kommerzielle Verwendungszwecke auf der offiziellen Website.

https://www.symantec.com/de/de/products/encryption

8

Machen Sie Ihre IT-Benutzerrichtlinien bekannt!

Grundsätze

Ohne verbindliche und verständliche IT-Benutzerrichtlinien können Ihre Mitarbeitenden nicht wissen, welche Handlungen erlaubt und welche verboten sind.
Regeln werden nur ernst genommen, wenn sich auch Vorgesetzte daran halten. Handeln Sie in allen Sicherheitsaspekten als Vorbild.

Erläuterungen:

- Definieren Sie schriftliche IT-Benutzerrichtlinien und lassen Sie diese von den Mitarbeitenden unterzeichnen.
- Machen Sie Sicherheit in Ihrem Unternehmen immer wieder und auf unterschiedliche Weise zum Thema.
- Führen Sie ein- bis zweimal pro Jahr Sensibilisierungsaktionen durch. Diese lassen sich auch mit einfachen Mitteln realisieren: z. B. durch E-Mails an alle Mitarbeitenden, Rundschreiben in der internen Post, Plakate in der Kantine, Beiträge in der Firmenzeitung usw.

Tipps & Tricks:

Richtlinien für die IT-Benutzerinnen und -Benutzer

- Regeln Sie die Installation und den Einsatz von eigenen Programmen und Hardware (Spiele, Bildschirmschoner, USB-Memory-Sticks, Modems, private Notebooks, Wireless LAN, Handheld-Computer etc.).
- Regeln Sie den Gebrauch des Internets: Was dürfen die Mitarbeitenden herunterladen, was nicht (Informationen, Programme etc.)?
- Untersagen Sie den Besuch von Chatrooms, aber auch von Webseiten mit pornografischen, rassistischen und gewaltverherrlichenden Inhalten.
- Legen Sie die Art und Weise der Datensicherung fest, v. a. bei den Notebookbenutzerinnen und -benutzern (siehe Punkt 2).
- Organisieren Sie eine Basisausbildung für alle Mitarbeitenden (z. B. gestützt auf diese Broschüre).
  Die wichtigsten Lernziele sind:
  - Der Nutzen der IT-Sicherheit
  - Bestimmen starker Passwörter
  - Sicherer Umgang mit Internet und E-Mail
  - Sicherer Umgang mit dem Virenschutz
  - Ablagestruktur von Dokumenten
- Papier allein genügt nicht! Mitarbeitende müssen für das Thema Sicherheit regelmässig sensibilisiert werden.
- Legen Sie den Umgang mit Passwörtern fest (siehe Punkt 6).
- Regeln Sie den Umgang mit Sicherheits-Updates und Antivirus-Programmen (siehe Punkt 3 und 5).
- Regeln Sie den Gebrauch von E-Mails: keine vertraulichen Daten übermitteln, kein Weiterleiten an die private E-Mail-Adresse, keine Kettenbriefe etc.
- Legen Sie den Umgang mit vertraulichen Informationen und Daten fest und richten Sie eine geschützte Dateiablage ein.
- Regeln Sie das Verhalten bei sicherheitsrelevanten Vorkommnissen, z. B. Viruswarnungen, Diebstählen und Verlusten von Notebooks und Passwörtern.

9

Schützen Sie die Umgebung Ihrer IT-Infrastruktur

Grundsätze

Wissen Sie, wer in Ihrem Unternehmen tagsüber ein und aus geht? Einige wenige Vorkehrungen verhindern bereits, dass Unbefugte an wichtige Geschäftsinformationen gelangen. Gelebte, sichtbare Sicherheit ist heute ein Qualitätskriterium und schafft Vertrauen bei Kunden und Lieferanten. Was nützt die beste Firewall, wenn sich Fremde in die Büroräume einschleichen können?

Erläuterungen:

- Alle Zugänge zum Gebäude resp. Firmenareal sind abzuschliessen oder zu überwachen. Falls dies nicht möglich ist, muss zumindest der Büroteil geschützt werden.
- Lassen Sie Besucher, Kunden und Bekannte nicht unbeaufsichtigt in Ihrem Betrieb umhergehen.
- Alle Drittpersonen werden am Empfang abgeholt, während ihres Aufenthaltes dauernd begleitet und beim Verlassen des Gebäudes am Ausgang wieder verabschiedet.
- Wenn Sie nicht über einen Empfang verfügen, der den Eingangsbereich überblickt, sollten Sie die Eingangstüre schliessen und ein Schild mit der Aufschrift «Bitte läuten!» anbringen.

Tipps & Tricks:

Richtlinien zum Thema IT-Umgebung

- Stellen Sie Server in abschliessbare, klimatisierte Räume. Ist kein entsprechender Raum verfügbar, schliessen Sie die Server in einen Computerschrank (Rack) ein.
- Lagern Sie brennbare Materialien wie Papier etc. nicht im oder unmittelbar vor dem Serverraum.
- Platzieren Sie im Serverraum einen gut sichtbaren CO_2-Feuerlöscher.
- Stellen Sie sicher, dass sämtliche Einstiegsmöglichkeiten (Fenster, Türen usw.) über einen ausreichenden Einbruchschutz verfügen. Entsprechende Informationsblätter sind auf jedem Polizeiposten erhältlich.
- Schlüssel und Badges müssen korrekt verwaltet und die entsprechenden Listen aktualisiert werden. Schlüssel mit Passepartout-Funktion sind restriktiv zu verteilen. Die entsprechenden Berechtigungen müssen mindestens jährlich auf ihre Notwendigkeit geprüft werden.
- Mitarbeitende, welche aus dem Unternehmen austreten, geben ihre Schlüssel, Badges und andere Zugangsberechtigungen beim Austritt ab.
- Stellen Sie Netzwerkdrucker nicht in öffentlich zugängliche Räume, da Unbefugte so Einblick in Dokumente erhalten können.
- Schliessen Sie Netzwerkkabel, die durch öffentliche Räume führen, sowie Modems, Hubs, Router und Switches ein.

10

Ordnen Sie Ihre Dokumente und Datenträger

Grundsätze

Hat Ordnung etwas mit Sicherheit zu tun? Mehr, als man auf den ersten Blick vielleicht meinen möchte.
Daten und Dokumente gehen auf einem ordentlichen Arbeitsplatz weniger verloren, als wenn die Arbeitsfläche mit Papieren, Handzetteln und Mäppchen übersät ist.

Erläuterungen:

- Eine klare Ordnungspolitik minimiert die Gefahr, dass sensible Dokumente im ungünstigsten Augenblick auftauchen oder von Unbefugten durch Zufall gelesen werden.
- Ordnung ist auch eine Frage des Images: Kunden oder Lieferanten schliessen bei einem Unternehmen vom ordentlichen Äussern gerne auf die innere Haltung.
- Ordnen Sie elektronische Daten und Papierdokumente in einem einheitlichen Ablagesystem, z. B. nach Kunden oder nach Projekten. Das System muss logisch aufgebaut und für die Mitarbeitenden gut verständlich sein.

Tipps & Tricks:

Richtlinien zum Thema Dokumente und Datenträger

- Löschen Sie nicht mehr benötigte elektronische Daten auf Speichermedien wie CDs, DVDs, Memory Sticks und Festplatten durch Überschreiben des gesamten Speicherbereichs. Der einfache Lösch-Befehl reicht nicht! Am besten werden Speichermedien vor der Entsorgung physisch zerstört.
- Halten Sie vertrauliche Unterlagen sowie Dokumente mit Personendaten konsequent unter Verschluss.
- Werden Speichermedien ausser Haus gegeben, sollten dafür neue und noch nie verwendete Datenträger eingesetzt werden. Konventionell gelöschte Informationen können relativ leicht wiederhergestellt und von Unbefugten gelesen werden. Eine zuverlässige Löschung der Daten kann nur mit einem «Wipe»-Programm erreicht werden. Informationen dazu sind im Internet erhältlich.
- Wenn Sie mit sensiblen Daten am Computer arbeiten, positionieren Sie den Bildschirm so, dass Kollegen und Besucher die Informationen nicht mitlesen können.
- Vernichten Sie nicht mehr benötigte Papierdokumente und Notizen mit sensiblen Daten sicher (Aktenvernichter).
- Sperren Sie während Pausen und bei Abwesenheit vom Arbeitsplatz den Computer mit einem Passwort und schliessen Sie vertrauliche Dokumente ein.
- Lassen Sie ausgedruckte Dokumente nicht auf dem Drucker liegen. Dies gilt insbesondere für öffentlich zugängliche Bereiche (Empfang usw.).

WIR, DIE GEBÄUDETECHNIKER.

NOI, I TECNICI DELLA COSTRUZIONE.

NOUS, LES TECHNICIENS DU BÂTIMENT.

Auskünfte
Für Auskünfte steht Ihnen der Verantwortliche IT-Betrieb von suissetec gerne zur Verfügung.
Tel. 043 244 73 44
Fax 043 244 73 79

Hinweis
Der Verein ISSS und suissetec übernehmen keinerlei Haftung für allfällige Schäden, die aus der richtigen oder falschen Anwendung des 10-Punkte-Programms entstehen.

Quellenangabe:
Dieses Merkblatt wurde durch den Verein ISSS (Information Security Society Switzerland), Bollwerk 21, CH-3001 Bern, Tel. 031 311 53 00, http://www.isss.ch, erarbeitet.

ISSS Information Security Society Switzerland

suissetec

Schweizerisch-Liechtensteinischer Gebäudetechnikverband
Auf der Mauer 11, Postfach, 8021 Zürich
T 043 244 73 00, F 043 244 73 79
www.suissetec.ch