Basler Versicherungen

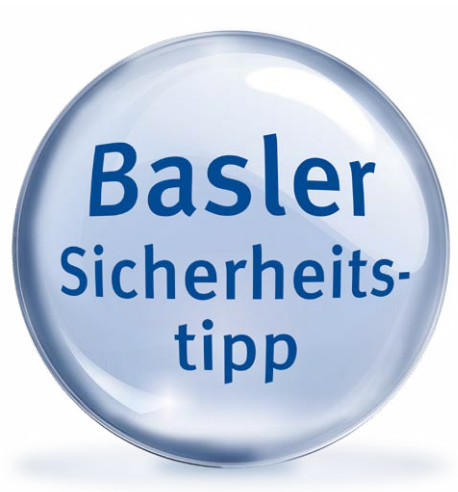
Sicherheitstipp Cyber-Schutz

Digitale Risiken bedrohen Ihr Unternehmen

Schützen Sie sich effektiv gegen Cyber-Gefahren

Zwei Drittel der Unternehmen in Deutschland waren in den Jahren 2016 und 2015 Cyber-Angriffen ausgesetzt.[1] Das zeigt eine Umfrage des Bundesamtes für Sicherheit in der Informationstechnik. Cyber-Attacken wie Datendiebstahl, Wirtschaftsspionage und Computerviren können demnach jedes Unternehmen treffen – unabhängig von seiner Größe.

Für kleine und mittelständische Unternehmen können digitale Risiken schnell existenzbedrohend werden. Umso wichtiger ist es, den eigenen Betrieb vor Cyber-Gefahren zu schützen. Mit unseren Sicherheitstipps können Sie digitalen Schäden effektiv vorbeugen und Cyber-Angriffe erfolgreich abwehren.

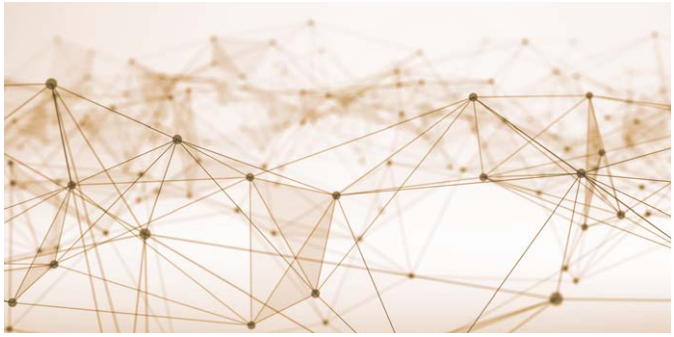


Organisatorischer Cyber-Schutz

„Zugriff verweigert“: Passwörter verhindern Datenklau

Die Arbeit am PC beginnt idealerweise mit der Eingabe eines Passworts. Passwörter schützen Ihr Computernetzwerk, Ihre IT-Anwendungen, Ihre E-Mail-Konten und andere Accounts vor unberechtigtem Zugriff. Sie sind das wichtigste Werkzeug, um Cyber-Kriminelle von sensiblen Daten fernzuhalten.

Leider gehen viele Mitarbeiter unvorsichtig mit Passwörtern um. Tagtäglich gelingen Cyber-Angriffe auf betriebliche IT-Systeme mit teils verheerenden Folgen, weil der Angreifer ein Passwort geknackt hat – zum Beispiel durch systematisches Ausprobieren, Ausspähen oder einfach durch Raten.



Unsere Sicherheitstipps

- Legen Sie für jeden Computer, jedes Konto und jede Anwendung ein anderes Passwort fest.
- Verwenden Sie komplexe Passwörter, die schwer zu knacken sind. Nutzen Sie idealerweise 16 Zeichen: kleine und große Buchstaben, Ziffern und Sonderzeichen.
- Verwahren Sie Passwörter sicher – auf keinen Fall unter der Tastatur oder im oberen Fach des Rollcontainers.
- Wechseln Sie Passwörter regelmäßig, mindestens alle 90 Tage.
- Speichern Sie keine Passwörter ab – weder auf programmierbaren Sondertasten noch durch Anmelderoutinen, bei denen Passwörter automatisch ergänzt werden.
- Verhindern Sie, dass Passwörter bei der Eingabe auf dem Monitor angezeigt werden.

1 Bundesamt für Sicherheit in der Informationstechnik (BSI): Ergebnisse der Cyber-Sicherheits-Umfrage 2016, 10. Oktober 2016, Seite 9

Ziehen Sie an einem Strang: Sicherheit geht alle an

Das beste Sicherheitskonzept ist wirkungslos, wenn Mitarbeiter es nicht umsetzen. Ihre Mitarbeiter sollten daher ein grundlegendes Verständnis für Cyber-Sicherheit entwickeln und digitale Gefahren eigenständig einschätzen können.

Es geht weniger darum, die Einhaltung strikter Richtlinien zu erzwingen. Vielmehr sollten sich Ihre Mitarbeiter mit der Frage auseinandersetzen, wie sie durch ihr eigenes Verhalten die Cyber-Sicherheit des Unternehmens beeinflussen und erhöhen können. Oftmals stellt sich dann von selbst ein Verständnis für einen umfassenden betrieblichen Cyber-Schutz ein.

Unsere Sicherheitstipps

- Erstellen Sie Richtlinien für die Handhabung von Hard- und Software, Passwörtern, personenbezogenen Daten, mobilen Endgeräten u. Ä. und vermitteln Sie diese an Ihre Mitarbeiter. Führen Sie ggf. Schulungen durch.
- Weisen Sie Ihre Mitarbeiter in den sicheren Umgang mit E-Mails und Anhängen von unbekannten Absendern ein.
- Erklären Sie den Schutz Ihrer IT-Systeme zur Chefsache und leben Sie praktische Cyber-Sicherheit vor. Gehen Sie mit gutem Beispiel voran, Ihre Mitarbeiter werden Ihnen folgen.

Technischer Cyber-Schutz

„Neues Update verfügbar“: Richten Sie ein Patch-Management ein

Computerprogramme sollten regelmäßig aktualisiert werden. Täglich werden neue Sicherheitslücken in Programmen entdeckt und veröffentlicht. Hacker nutzen diese Schwachstellen, um sich Zugriff auf IT-Systeme zu verschaffen und dort großen Schaden anzurichten.

Programmhersteller schließen Sicherheitslücken üblicherweise zügig. Damit Ihr IT-System optimal geschützt ist, müssen Sicherheitsupdates (Patches) unverzüglich eingespielt werden. Ein strukturiertes Patch-Management stellt sicher, dass alle Programme jederzeit auf dem aktuellsten Stand sind.

Unsere Sicherheitstipps

- Erstellen Sie ein Verzeichnis aller Programme, die Sie verwenden.
- Prüfen Sie, für welche Programme Sie automatisch regelmäßige Updates erhalten.
- Erstellen Sie eine Übersicht, für welche Programme Sie selbst Updates einspielen müssen. Installieren Sie verfügbare Updates unverzüglich.
- Informieren Sie sich regelmäßig über bekannt gewordene Sicherheitslücken, z. B. mithilfe von Newslettern oder Branchenplattformen.
- Prüfen und testen Sie das Einspielen von Sicherheitsupdates regelmäßig. Nur ordnungsgemäß installierte Updates bieten ausreichenden Schutz.

„Eindringling gefunden“:
Installieren Sie Antivirensoftware und Firewalls

Antivirenprogramme schützen Ihren Betrieb vor Schadsoftware. Sie verhindern, dass sich Viren in Ihr IT-System einschleusen, dort Schaden anrichten und sich selbstständig vermehren. Firewalls sichern Ihr Unternehmen gegen unberechtigte Zugriffe von außen. Antivirenprogramme und Firewalls müssen immer auf dem aktuellsten Stand sein, um Ihren Betrieb effektiv gegen Cyber-Bedrohungen schützen zu können.

Innerhalb größerer Netzwerke ist es sinnvoll, Teilnetze einzurichten. Teilnetze mit besonders sensiblen Daten (z. B. Kundeninformationen) können so effektiver geschützt werden. Sie sind dann nicht nur gegen Angriffe aus dem Internet, sondern auch gegen Angriffe aus anderen, eventuell infizierten Teilnetzen gesichert.

Unsere Sicherheitstipps

- Verwenden Sie ausschließlich aktuelle Antivirenprogramme und Firewalls. Spielen Sie verfügbare Updates unverzüglich ein.
- Prüfen Sie Ihr IT-System mindestens einmal pro Woche vollständig mithilfe eines Antivirenprogramms auf Schadsoftware.
- Überwachen Sie die Funktionen Ihrer Firewall und passen Sie die Einstellungen den Sicherheitsbedürfnissen Ihres Unternehmens an.
- Verwenden Sie nur Programme aus vertrauenswürdigen Quellen. Deinstallieren Sie unnötige Programme und Anwendungen.
- Antivirenprogramme und Firewalls sind ein Basisschutz. Gegen bestimmte Arten von Schadsoftware wie z. B. Ransomware bieten sie oftmals keine ausreichende Sicherheit. Lassen Sie sich hierzu professionell beraten.

Weniger ist manchmal mehr: Legen Sie Nutzerrechte fest

Eine goldene Regel zur Cyber-Sicherheit lautet: „so viel wie nötig und so wenig wie möglich“ (Need-to-know-Prinzip). Jeder Mitarbeiter sollte demnach nur auf Daten zugreifen und Programme ausführen dürfen, die er für seine tägliche Arbeit braucht.

Insbesondere sollten Mitarbeiter keine Administrationsrechte besitzen, wenn sie diese nicht tatsächlich benötigen. Bei einer unsachgemäßen Bedienung oder einem Hackerangriff auf dieses Konto können sonst erhebliche Schäden entstehen. Ausgebildete Systemadministratoren passen die Zugriffsrechte und Befugnisse jedes Mitarbeiters individuell auf dessen Arbeitsbereich an.

Unsere Sicherheitstipps

- Stellen Sie sicher, dass jeder Mitarbeiter ein eigenes, passwortgeschütztes Benutzerkonto mit eingeschränkten Rechten hat.
- Vergeben Sie Administrationsrechte nur an Mitarbeiter, die diese tatsächlich benötigen.
- Prüfen Sie in regelmäßigen Abständen, ob die vergebenen Rechte noch zeitgemäß sind oder angepasst werden müssen.
- Löschen oder deaktivieren Sie nicht mehr benötigte Benutzerkonten.
- Erlauben Sie keine anonymen oder von mehreren Personen gemeinsam genutzten Konten.

„Ihr System wird neu gestartet“: Erstellen Sie regelmäßig Back-ups

Systemabstürze, Programmfehler, technische Probleme, versehentliches Löschen oder gar ein Angriff durch einen Verschlüsselungstrojaner – all dies kann dazu führen, dass wichtige Daten verloren gehen. Nur eine regelmäßige Datensicherung (Back-up) verhindert einen unwiderruflichen Datenverlust. Besonders kleine und mittelständische Unternehmen können den Ausfall ihrer IT-Systeme und den Verlust ihrer Daten finanziell nur schwer verkraften.

Viele kleinere Betriebe sichern ihre Daten jedoch immer noch manuell in unregelmäßigen Abständen. Das ist zum einen mühsam, zum anderen können dabei schnell Daten übersehen werden. Oft entfällt die Datensicherung aus Zeitmangel ganz. Automatisierte Back-ups verlaufen nach vorher festgelegten Routinen und stellen sicher, dass die Daten nach einem Notfall schnell wieder verfügbar sind.

Unsere Sicherheitstipps

- Sichern Sie alle Daten des laufenden Betriebs mit einem automatisierten Back-up-Programm – mindestens 1x täglich.
- Bewahren Sie Back-ups physisch getrennt von den gesicherten Systemen auf. Der Aufbewahrungsort sollte gegen Elementarschäden (Wasser, Feuer, Blitz) und Diebstahl geschützt sein.
- Üben Sie das Einspielen von Back-ups regelmäßig – damit die Daten im Notfall zügig wiederhergestellt werden können.
- Prüfen Sie das Back-up regelmäßig auf seine Funktionsfähigkeit. Berücksichtigen Sie hierbei die begrenzte Lebensdauer von Datenträgern (Festplatten/ USB-Sticks: ca. 10 Jahre).

Nichts geht mehr: Entwickeln Sie ein Notfallkonzept und Sicherheitsrichtlinien

Jedes Unternehmen benötigt eigene Sicherheitsrichtlinien und ein Notfallkonzept – egal ob Kleinbetrieb oder Mittelständler. Sicherheitsrichtlinien enthalten genaue Vorgaben für Ihre Mitarbeiter zum Schutz der betrieblichen IT-Systeme. Sie regeln z. B. den Umgang mit sensiblen Daten, E-Mails, privater Internetnutzung und mobilen Endgeräten. Sicherheitsrichtlinien sollten verständlich formuliert sein, sodass Ihre Mitarbeiter die Vorgaben verstehen und einhalten können.

Selbst die besten Sicherheitsrichtlinien können einen IT-Notfall nicht vollständig verhindern. Kommt es aufgrund eines Hackerangriffs oder aggressiver Schadsoftware zu einem Systemausfall, muss schnell gehandelt werden. Jeder Ausfalltag kostet bares Geld und kann schnell existenzbedrohend werden. In einem Notfallkonzept sind wichtige Informationen zur Krisenbewältigung festgehalten. Es klärt Prioritäten, legt Sicherheitsziele und -maßnahmen fest und regelt Zuständigkeiten. Checklisten nennen die wichtigsten Handlungsschritte im Krisenfall.

Unsere Sicherheitstipps

- Erstellen Sie eigene Sicherheitsrichtlinien und ein Notfallkonzept mit genauen, selbsterklärenden Anleitungen für Ihre Mitarbeiter.
- Händigen Sie jedem Mitarbeiter die Sicherheitsrichtlinien und das Notfallkonzept aus. Stellen Sie sicher, dass die Vorgaben verstanden werden. Veranstalten Sie ggf. einen begleitenden Workshop.
- Überprüfen Sie die Sicherheitsrichtlinien und das Notfallkonzept regelmäßig auf Vollständigkeit und Aktualität. Passen Sie diese ggf. an neue Entwicklungen an.
- Testen Sie die Sicherheitsrichtlinien und das Notfallkonzept regelmäßig, z. B. anhand typischer Geschäftsabläufe oder simulierter Notfälle. Lassen Sie Ihre Mitarbeiter daran teilnehmen und führen Sie Nachbesprechungen durch.

Basler Versicherungen
Basler Str. 4, 61345 Bad Homburg

BAS 3467 07.17 WMD