

SECURITY **[SNAPSHOT]**

Checkliste: Vom Sicherheitsrisiko Mitarbeiter zum Sicherheitsfaktor

87.800 \$

beträgt der durchschnittliche finanzielle Schaden einer Datenschutzverletzung für kleine und mittelständische Unternehmen.¹

992.000 \$

beträgt der durchschnittliche finanzielle Schaden einer Datenschutzverletzung für Großunternehmen.²

46 %

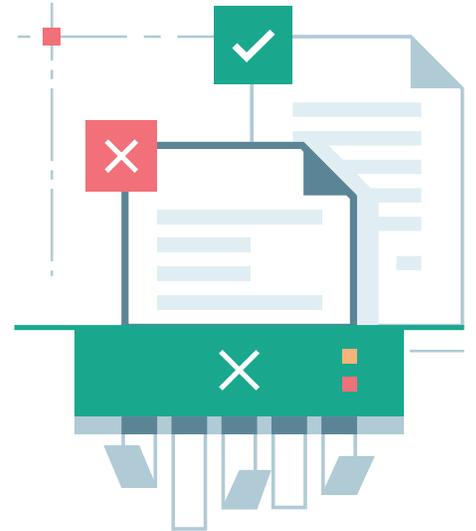
der Sicherheitsvorfälle werden durch leichtsinnige oder unwissende Mitarbeiter verursacht.³

35 %

der Unternehmen werden versuchen, Sicherheitsschwachstellen durch Mitarbeiterschulungen zu reduzieren.⁴

61 %

der C-Level-Führungskräfte außerhalb der IT geben an, dass Datensicherheit eines der wichtigsten IT-Sicherheitsthemen ist.⁵

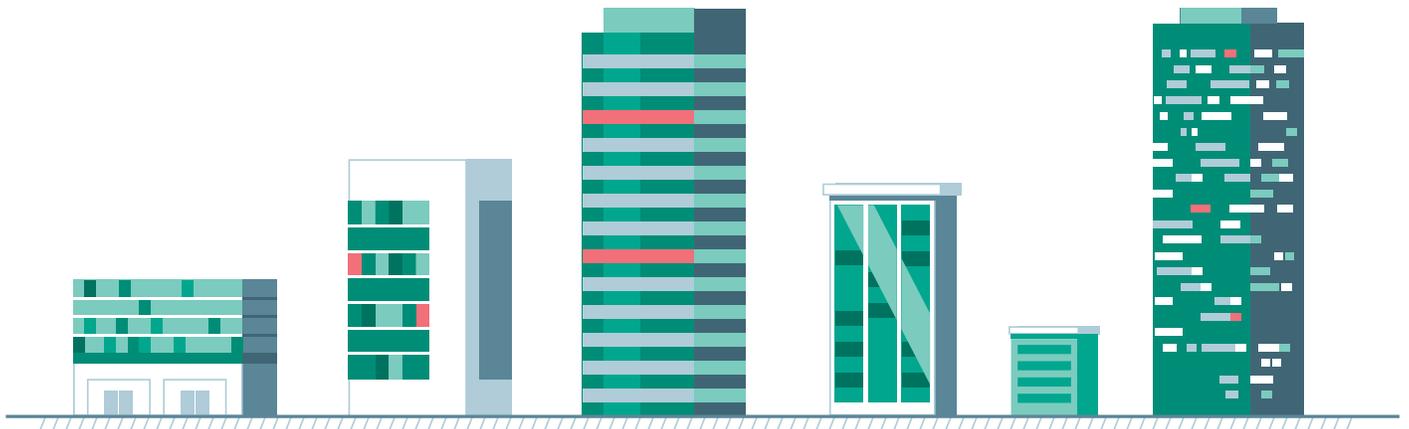


1-5: Globale Umfrage zu IT-Sicherheitsrisiken 2017 von Kaspersky Lab und B2B International

Die Bedrohung innerhalb Ihres Unternehmens

Wenn Sie sich in Ihrem Unternehmen umsehen, erkennen Sie direkt eine der größten IT-Sicherheitsbedrohungen: die Menschen, mit denen Sie arbeiten. Denn selbst Mitarbeiter ohne jede böswillige Absicht und mit hohem Engagement für Ihr Unternehmen können versehentlich vertrauliche Daten offenlegen oder Malware ins System lassen, die in Ihrem Netzwerk Chaos anrichtet.

Diese interne Bedrohung stellt für Unternehmen aller Größen eine fortwährende Herausforderung dar und lässt sich nur schwer vorhersagen. Denn Mitarbeiter nutzen heute verschiedenste Geräte – oft sogar an unterschiedlichen Standorten – und Ihre IT-Abteilung hat dabei die schwierige Aufgabe, bewegliche Ziele zu überwachen. Doch mit folgenden Schritten können Sie sicherstellen, dass Ihr Unternehmen geschützt ist. Indem Sie das Problem der IT-Sicherheit von allen Seiten betrachten, können Sie das ideale Gleichgewicht zwischen dem nötigen Mitarbeiterzugriff und der gewünschten Datensicherheit finden.



10 Tipps für umfassende Sicherheit

1. Ihre Mitarbeiter sind Ihre erste Verteidigungslinie.

ERKLÄRUNG:

In jedem Unternehmen gilt: Je besser Ihre Mitarbeiter wissen, wie sie zum Schutz Ihres Unternehmens beitragen können, desto sicherer ist es. Stellen Sie sicher, dass alle Mitarbeiter die Sicherheitsrichtlinien Ihres Unternehmens kennen und einhalten. Bringen Sie die Richtlinien gut sichtbar an und beantworten Sie regelmäßig Fragen Ihrer Mitarbeiter.

2. Mitarbeiterschulungen sind den Aufwand wert.

ERKLÄRUNG:

80 Prozent der Cybervorfälle beginnen mit menschlichen Fehlern. Sie können diesen Prozentsatz jedoch reduzieren, indem Sie Mitarbeiter hinsichtlich der Gefahren schulen, die insbesondere von Social-Engineering-Angriffen ausgehen. Mithilfe von Phishing, Ransomware und Spear Phishing verschaffen sich Cyberkriminelle über Ihre Mitarbeiter Zugang zu Ihrem Unternehmen. Laut den Daten von Kaspersky Lab können Unternehmen, die ihre Angestellten hinsichtlich Cybersicherheit schulen, in 93 Prozent der Fälle davon ausgehen, dass ihre Mitarbeiter das Gelernte auch anwenden. Schulungen haben die gewünschte Wirkung, insbesondere wenn vielfältige und kreative Methoden angewandt werden. Präsenztrainings gepaart mit Webinaren, Infografiken und Videos vermitteln die nötige Botschaft.

3. Die Schulung Ihrer Mitarbeiter beginnt ganz oben: mit den Führungskräften Ihres Unternehmens.

ERKLÄRUNG:

Die meisten Führungskräfte wissen, dass Cybersicherheit ein wichtiges Thema ist. Viele wissen jedoch nicht, wie wichtig hierbei ihre eigene Rolle ist. Indem Sie schon auf Managementebene eine Unternehmenskultur der Cybersicherheit fördern, können Führungskräfte nicht nur gewährleisten, dass ihre Mitarbeiter das Thema Sicherheit ernst nehmen, sondern auch zum Schutz Ihres Unternehmens beitragen. Darüber hinaus wissen viele Vorstände, dass sie bei Angriffen häufig rechtlich belangt werden können und oft die Einhaltung ihrer Sorgfaltspflicht beim Schutz von Kunden und Assets nachweisen müssen. Wenn Sie dieses Thema bei Führungskräften ansprechen, dürfen Sie nicht einfach davon ausgehen, dass Ihr Gegenüber die Probleme rund um IT-Sicherheit kennt. Indem Sie Wissenslücken schließen, können sie die Komplexität dieses Themas besser verstehen und das Sicherheitsbewusstsein in Ihrem Unternehmen fördern.

4. Alle Mitarbeiter müssen wissen, wie sie die IT-Abteilung über Sicherheitsvorfälle informieren können.

ERKLÄRUNG:

Gehen Sie mit Mitarbeitern die Anzeichen für eine Sicherheitsverletzung durch und teilen Sie ihnen mit, wen sie in solchen Fällen kontaktieren müssen. Telefonnummern und Kontakte sollten deutlich sichtbar aufgehängt werden. Viele Mitarbeiter melden einen solchen Fall nur zögerlich, doch ihre Wachsamkeit ist essenziell für den Schutz Ihres Unternehmens. Deshalb sollten sie sich schon im Zweifelsfall an die IT-Abteilung wenden, um verdächtige Aktivitäten zu melden.

- 5.** Behalten Sie die Kontrolle über die Benutzerzugriffsrechte.

ERKLÄRUNG:

Einer der wichtigsten Aspekte für Ihre IT-Abteilung ist die Kontrolle darüber, wer auf bestimmte Programme, Geräte und vertrauliche Informationen innerhalb des Unternehmens zugreifen kann. Hierzu muss sie die verschiedenen Rollen kennen und den Zugriff auf bestimmte Mitarbeiter beschränken und kann so den Schutz deutlich erhöhen.

- 6.** Zeichnen Sie alle Berechtigungen auf.

ERKLÄRUNG:

Bei einem Sicherheitsvorfall können Sie viel Zeit sparen, wenn Sie schon vorab wissen, welche Nutzer auf welche Bereiche Ihres Unternehmens zugreifen können. Indem Sie alle Zugriffsrechte und Benutzerberechtigungen aufzeichnen, ersparen Sie Ihrer IT-Abteilung viel Zeit und Aufwand und ermöglichen eine schnelle Wiederherstellung.

- 7.** Führen Sie regelmäßig Scans durch, um Systemschwachstellen zu identifizieren, und halten Sie Netzwerkdienste auf dem neuesten Stand.

ERKLÄRUNG:

Ihre Systeme und Ihr Netzwerk verändern sich ständig. Durch neue Mitarbeiter und anhaltende Nutzung müssen immer wieder neue Geräte und Programme überprüft werden. Darüber hinaus benötigen Benutzer oft neue Tools, um ihre Aufgaben zu erledigen, wodurch wiederum neue Geräte und Programme in Ihr Netzwerk integriert werden. In einem solchen Szenario ist es entscheidend, durch regelmäßige Scans Ihres gesamten Systems Schwachstellen zu identifizieren.

- 8.** Wenn Sie anfällige Netzwerkdienste und -programme finden, erwägen Sie neue Richtlinien.

ERKLÄRUNG:

Bei Netzwerkskans werden häufig unerwartete Schwachstellen aufgedeckt. Nach diesen Scans müssen Sie abwägen, ob Ihre Richtlinien und Prozesse aktualisiert werden müssen, um den Schutz zu wahren.

- 9.** Aktualisieren Sie anfällige Komponenten und Programme.

ERKLÄRUNG:

Anbieter stellen regelmäßig Patches für anfällige Komponenten und Programme bereit, um gefundene Schwachstellen zu schließen. Die Anwendung dieser Patches ist essentiell und kann in vielen Fällen über einen wöchentlichen Updatezeitplan erfolgen.

- 10.** Installieren Sie eine mehrschichtige Sicherheitslösung.

ERKLÄRUNG:

Menschliche Fehler lassen sich nie vollständig ausschließen. Doch mithilfe einer mehrschichtigen Sicherheitslösung können Sie Bedrohungen aus unterschiedlichen Perspektiven untersuchen. Deshalb ist eine solche Lösung eine unerlässliche Komponente für Ihre Sicherheitsstrategie.

True Cybersecurity for Business

True Cybersecurity von Kaspersky Lab kombiniert mehrschichtige Sicherheit mit Cloud-basierten Bedrohungsinformationen und lernfähigen Systemen, damit Sie vor Cyberrisiken geschützt sind. True Cybersecurity verhindert Angriffe nicht nur, sondern kann sie auch vorhersagen, erkennen und schnell abwehren und gewährleistet so die Geschäftskontinuität.

Über Kaspersky Lab

Kaspersky Lab ist einer der weltweit am schnellsten wachsenden IT-Sicherheitsanbieter und der weltweit größte Privatanbieter von Sicherheitslösungen. Das Unternehmen rangiert unter den vier Top-Anbietern von Sicherheitslösungen für Endpoint-Benutzer (IDC, 2014). Seit seiner Gründung im Jahr 1997 hat Kaspersky Lab stets eine Vorreiterrolle bei der IT-Sicherheit gespielt und bietet großen Unternehmen, KMUs und Heimanwendern zuverlässige digitale Lösungen. Kaspersky Lab ist ein internationales Unternehmen, das weltweit in fast 200 Ländern und Regionen tätig ist und bei über 400 Millionen Benutzern für Schutz sorgt.

Hier erfahren Sie mehr über Cybersicherheit: de.securelist.com

www.kaspersky.de
[#truecybersecurity](https://twitter.com/truecybersecurity)

Kaspersky Labs GmbH,
Despag-Straße 3, 85055 Ingolstadt, Deutschland
Tel: 866-563-3099 | E-Mail: salesdach@kaspersky.com

© 2017 Kaspersky Labs GmbH. Alle Rechte vorbehalten. Eingetragene Markenzeichen und Handelsmarken sind das Eigentum ihrer jeweiligen Rechtsinhaber. Microsoft, Windows Server und SharePoint sind entweder eingetragene Marken oder Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

