ToasterNET

IT-SERVICE .NETWORK

IT-Sicherheit

Worauf es beim Thema IT-Sicherheit wirklich ankommt – und wie Sie Ihr Unternehmen zuverlässig schützen

Vorwort

Fast täglich erscheinen Berichte über neue Erpressungstrojaner, IT-Sicherheitslücken oder Hackerangriffe. Die Unternehmensgröße spielt für die Cyberkriminellen dabei keine Rolle: Kleine und Mittelstandsunternehmen sind von Angriffen genauso betroffen, wie große Konzerne.

Dass sich die Angriffe auf IT-Umgebungen derart häufen, liegt auch daran, dass Cyberkriminalität weiterhin ein lukratives Geschäft für die Angreifer ist. Doch die Abwehr von Hackerangriffen wird immer schwerer. Unternehmen und IT-Dienstleister müssen sich daher auf einen neuen Bedarf an Sicherheitslösungen einstellen.

Um Ihre sensiblen Firmendaten zu schützen, bedarf es deshalb eines durchdachten IT-Sicherheitskonzepts, das regelmäßig von IT-Sicherheitsexperten angepasst wird und auf anerkannten Normen und individuellen Anforderungen basiert.

Lernen Sie in diesem Whitepaper,

- Welche Sicherheitsrisiken es für Ihre IT gibt,
- Wie Sie Social Engineering vorbeugen können,
- Worauf Sie bei der Passwortwahl achten sollten.

Für individuelle Fragen und Beratungen zu Sicherheitskonzepten und -Lösungen für Ihr Unternehmen stehen wir Ihnen gern zur Verfügung.

Inhaltsverzeichnis

1. Die größten IT-Sicherheitsrisiken: Datenklau, Ransomware & Co.

Ganz gleich, ob es sich um ein kleines oder mittelständisches Unternehmen oder einen großen Konzern handelt: Vor IT-Sicherheitsrisiken ist niemand gefeit. Zu den größten Gefahren für die Unternehmens-IT gehören dabei Datenklau, Ransomware (bzw. andere Schadsoftware) und Hardware-Defekte. Jede dieser Gefahrenquellen erfordert bestimmte Maßnahmen und Vorgehensweisen, um Schäden zu vermeiden oder zumindest zu verringern.

Ein Backup schützt vor Angriffen mittels Ransomware. Angreifer verschlüsseln dabei die Daten auf einer Festplatte oder einem Server und geben sie nur gegen ein Lösegeld (Ransom) wieder frei. Wer eine gute Backup-Strategie hat, ist aber nicht zwingend an die Lösegeldzahlung gebunden, sondern kann die Daten in der Regel – wenn auch mit einigem Aufwand – wiederherstellen.

Auch wenn es nervt: Regelmäßige Updates & Backups schützen die IT vor Datenverlust und Ausfällen.

Generell gehören Ransomware und Phishing-Angriffe zu den erfolgreichsten Cyber-angriffen – und den lukrativsten. Mithilfe solcher Attacken können Hacker leicht an wertvolle Unternehmensdaten gelangen und diese im Darknet verkaufen. Besonders beliebt sind dabei auch Passwörter und Login-Daten, die ebenfalls für Angriffe genutzt werden.

Oft sind dabei jedoch nicht mal die Technologien an sich gefährdet. Stattdessen sind es immer wieder die Mitarbeiter, die das größte Sicherheitsrisiko darstellen. Das belegen auch zahlreiche Studien, in denen gleichzeitig vor Angriffen mittels Social Engineering gewarnt wird.

2. Sicherheitsrisiko Mensch: Social Engineering

60 Prozent der IT-Sicherheitsvorfälle in Unternehmen gehen auf den Faktor Mensch zu-rück – Tendenz steigend. Das machen sich sogenannte Social Engineers zunutze, die Schwachstellen in der IT-Sicherheit gekonnt ausnutzen. Unter Social Engineering versteht man einen Trickbetrug bzw. eine soziale Manipulation. Offline sind die Social Engineers auch als Hochstapler bekannt; im Internet fallen sie in die Kategorie der Cyberkriminellen. Der Schutz vor Social Engineering sollte daher bei jedem Unternehmen zum Sicherheits-konzept gehören.

Social Engineering kann viele Gesichter haben. Zu den bekanntesten – und wohl auch den effektivsten – Social-Engineering-Methoden gehören die Phishing-Mail und der CEO-Betrug (CEO-Fraud). Nichtsahnende Nutzer und Mitarbeiter sollen darüber so beeinflusst werden, dass sie vertrauliche Informationen preisgeben und den Angreifern so Tür und Tor zu sensiblen Unternehmensdaten, Netzwerk-Passwörtern oder gar Firmenkonten öffnen. Dafür spionieren die Cyberkriminellen das persönliche und betriebliche Umfeld ihrer Opfer aus, täuschen Identitäten vor oder nutzen Verhaltensweisen wie Autoritätshörigkeit aus.

Die beliebtesten Methoden der Cyberkriminellen beim Social Engineering auf einen Blick

1.

Der „vergessene“ USB-Stick

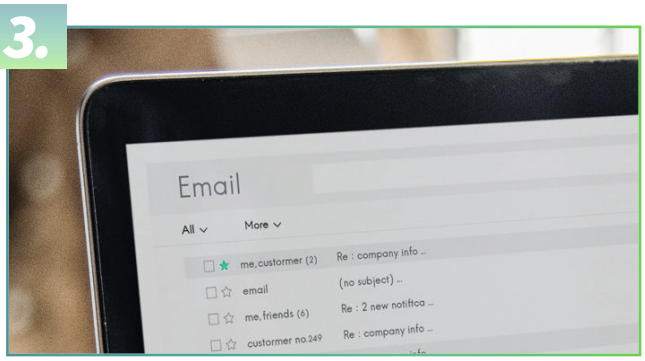
(Augenscheinlich vergessene externe Medien, auf denen sich Schad- / Spionagesoftware befindet)

2.

Phishing-Mails

(Mails, die zum Ziel haben, einen Link zu klicken oder Kontoinformationen einzugeben)

3.



Spear-Phishing

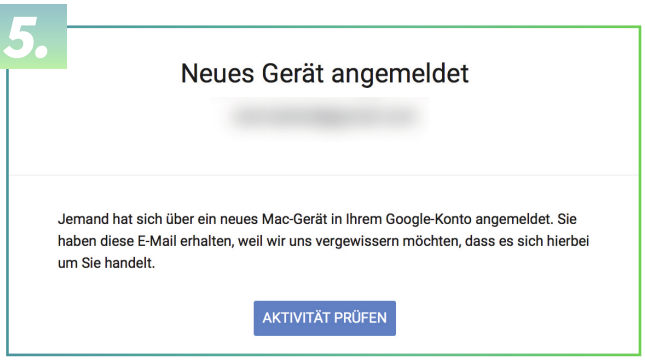
(Maßgefertigte Phishing-Mails an einzelne oder kleine Gruppen von Menschen)

4.

Phishing per Telefonanruf

(Anrufe falscher Support-Mitarbeiter, etc.)

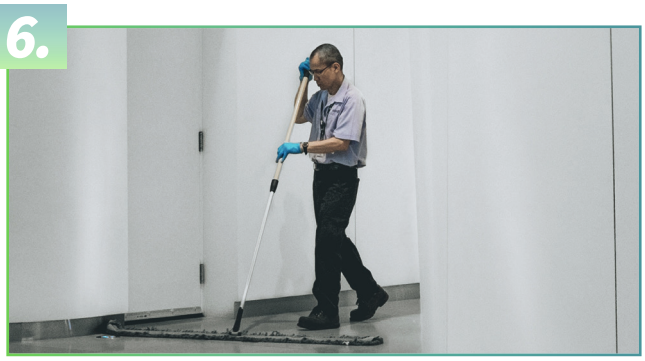
5.



Gehackte Webmail-Konten,

die als Archiv genutzt werden

6.



Unbefugtes Eindringen

in Firmengebäude / Büros

Schutz vor Social Engineering

Da Social Engineering zu den häufigsten Angriffsformen zählt, ist die Sensibilisierung Ihrer Mitarbeiter wichtig. Führen Sie Schulungen zum Thema durch und geben Sie Ihren Mitarbeitern einige wichtige Grundregeln an die Hand, mit denen Sie sie auf die wachsende Gefahr des Social Engineerings aufmerksam machen.

1. Geben Sie keine vertraulichen Informationen in sozialen Netzwerken preis. Sorgen Sie für die Verschlüsselung sensibler Daten auf Ihrem PC.

2. Teilen Sie keine Passwörter, Zugangsdaten oder Kontoinformationen per E-Mail oder Telefon mit. Hinterfragen Sie wenn nötig das Anliegen unbekannter Anrufer.

3. Prüfen Sie E-Mails von unbekannten Absendern genau auf Ihre Legitimität und lassen Sie Vorsicht beim Umgang mit ihnen walten.

4. Nutzen Sie für den Login immer nur die tatsächliche Login-Seite, nicht aber die Login-Aufforderungen und -Links aus E-Mails.

5. Gehen Sie verantwortungsvoll mit Ihren Daten in sozialen Netzwerken um und prüfen Sie regelmäßig Ihre Datenschutzeinstellungen bei Facebook, Twitter & Co.

6. Bewahren Sie sensible Unternehmensdaten sicher auf, sperren Sie Ihren Rechner, wenn Sie ihn verlassen und schreddern Sie nicht mehr benötigte Dokumente.

7. Legen Sie Richtlinien für den Umgang mit Wechseldatenträgern wie USB-Sticks und CDs in Ihrem Unternehmen fest. Fremde Datenträger können ein großes Sicherheitsrisiko sein!

3. Passwortsicherheit – darauf kommt es an

Ganz gleich, ob Computerzugang, E-Mail-Account oder Social-Media-Profil: Wir benötigen in unserem Alltag immer mehr Passwörter, um unsere sensiblen Daten zu schützen. Doch die tägliche Passwortflut nervt die Deutschen. Kein Wunder also, dass immer noch viele User einfach zu merkende (und zu erratende!) Passwörter oder das gleiche Kennwort für mehrere Accounts nutzen.

Die 10 beliebtesten Passwörter (Stand: 2018, Quelle: t3n)

123456	*hallo123*
12345	*hallo*
123456789	*123*
ficken	*passwort*
12345678	*master*

Was bereits bei privaten Accounts schnell gefährlich werden kann, ist bei Unternehmenskonten grob fahrlässig: Hacker haben so leichtes Spiel, an geheime Unternehmensdaten zu kommen und diese für ihre Zwecke zu nutzen. Umso wichtiger ist es also, dass auch in Unternehmen regelmäßig auf das Thema Passwortsicherheit aufmerksam gemacht wird.

So ist es sinnvoll, konkrete Regelungen zur Wahl eines sicheren Passworts aufzustellen und dafür zu sorgen, dass sich die Mitarbeiter auch daran halten. Auch Schulungen zum Thema Passwortwahl und -sicherheit können für eine höhere Awareness bei den Mitarbeitern sorgen.

3.1 Was macht ein sicheres Passwort aus?

Grundsätzlich ist kein Passwort zu 100 Prozent sicher. Es gibt aber einige Richtlinien, die dabei helfen können, Accounts besser vor Passwortdiebstahl zu schützen. Dazu gehört in jedem Fall der regelmäßige Wechsel der Passwörter. Dieser macht es Hackern schwerer, in die Accounts einzudringen. Werden Fälle bekannt, bei denen Datenbanken gehackt wurden, ist es meist schon zu spät. Dann sind die gestohlenen Passwörter nämlich bereits im Umlauf und Hacker können im schlimmsten Fall ungehindert Zugriff auf die Daten nehmen.

Damit ein Passwort als »sicher« gilt, sollte es einige Voraussetzungen erfüllen:

- ✓ **Umfasst mindestens 10 Zeichen**
- ✓ **Besteht aus einer Kombination aus Groß- und Kleinbuchstaben**
- ✓ **Beinhaltet Sonderzeichen und Zahlen**

Passwörter richtig verwalten

Dafür gelten die vier folgenden Regeln:

- *Passwörter dürfen niemals im Klartext abgespeichert werden.*
- *Passwörter sind mit anerkannten Verfahren zu hashen (z.B. SHA-256).*
- *Passwörter sind vor dem Hashen mit einer zufälligen Zeichenfolge zu versehen (dem Salt), um die systematische Rückführung von Hashes zu erschweren.*
- *Passwörter sollten von einer Mehr-Faktor-Authentifizierung begleitet werden.*

Um die Passwortverwaltung zu vereinfachen, ist zudem der Einsatz eines Passwortmanagers sinnvoll.

3.2 Passwortmanager & Passwortmanagement

Passwortmanager sind ein besonders nützliches Tool, um sämtliche Kennwörter in einer einzigen, verschlüsselten Datei zu speichern. Statt sich jedes einzelne Passwort zu merken, muss man nur noch ein einziges Kennwort zur Hand haben: das sogenannte Masterkennwort. Die meisten Passwortmanager bieten eine Browser-Extension an, sodass in vielen Fällen die Eingabefelder auf Login-Seiten automatisch mit dem abgespeicherten Kennwort ausgefüllt werden. Empfehlenswerte Passwortmanager sind zum Beispiel:

- Dashlane Premium
- Intel Security True Key Premium
- Keeper Security
- Lastpass Premium

Zusätzlich bieten viele Passwortmanager die Möglichkeit, neue Passwörter zu generieren. Diese folgen dabei automatisch den geltenden Sicherheitsregeln. Alternativ kann man festlegen, welche Zeichen auf jeden Fall enthalten sein sollten. Außerdem lässt sich mithilfe eines guten Passwortmanagers unkompliziert überprüfen, ob die genutzten Passwörter sicher sind oder hier Nachbesserungsbedarf besteht.

Langes Suchen nach Login-Daten während eines Meetings kann ganz schön peinlich sein. Ein Passwortmanager schafft hier Abhilfe.

4. DSGVO: Neues Gesetz, neue Risiken?

Seit dem 25. Mai 2018 gilt die EU-Datenschutzgrundverordnung – kurz DSGVO. Damit endete eine zweijährige Übergangsfrist, die Unternehmen genug Zeit gegeben haben sollte, um die Anforderungen der DSGVO zu erfüllen. Trotzdem waren kurz vor der Deadline längst nicht alle Unternehmen mit der Umsetzung fertig: Gerade einmal 32 Prozent der deutschen Unternehmen hatten zum Inkrafttreten des neuen Datenschutzgesetzes alle Anforderungen größtenteils umgesetzt.

Bis heute herrscht vielerorts noch immer Unsicherheit. Welche Maßnahmen müssen Unternehmen jetzt ergreifen, um auf der rechtssicheren Seite zu sein? Und was bringt die EU-Datenschutzgrundverordnung überhaupt?

Aufgabe der EU-Datenschutzgrundverordnung

»Die Datenschutzgrundverordnung ist eine Verordnung der Europäischen Union, mit der die Regeln für die Verarbeitung von personenbezogenen Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht werden. Dadurch soll einerseits der Schutz von personenbezogenen Daten innerhalb der Europäischen Union sichergestellt, andererseits der freie Datenverkehr innerhalb des Europäischen Binnenmarktes gewährleistet werden.« (Quelle: Wikipedia)

Bereits vor Inkrafttreten der DSGVO war der Datenschutz eindeutig geregelt – und zwar mit dem Bundesdatenschutzgesetz (BDSG). Allerdings geht die neue EU-Datenschutzverordnung in einigen Passagen über das BDSG hinaus. So sind personenbezogene Daten zum Beispiel bereits dann verletzt, wenn Sie deren Verfügbarkeit nicht gewährleisten können. Außerdem werden die Dokumentationspflichten und Betroffenenrechte ausgeweitet und die Bußgelder deutlich erhöht. So drohen bei Nichteinhaltung der DSGVO Strafen von bis zu 20 Millionen Euro bzw. vier Prozent des weltweiten Umsatzes des betroffenen Unternehmens.

4.1 Neue Risiken durch die DSGVO?

Datenschutz steht nicht nur dank der neuen EU-Datenschutzgrundverordnung immer mehr im Fokus. Vor allem im Hinblick auf Datenpannen durch Sicherheitslücken oder Hackerangriffe wird die Datensicherheit auch immer mehr zum Cyberrisiko. Kommen personenbezoge Daten abhanden, sind die finanziellen Schäden für Unternehmen enorm. Je nach Umfang der Datenpanne betragen die Kosten für ein Datenleck mittlerweile rund 3,9 Millionen Euro. Darunter fallen Kosten für die Wiederherstellung der Daten, aber auch die Arbeitsstunden, die Unternehmen zum Eindämmen der Datenpanne aufwenden müssen. Dazu kommen die angesprochenen Bußgelder von bis zu 20 Millionen Euro, die von den Aufsichtsbehörden verhängt werden.

Unternehmen müssen sich bewusst sein, dass das Risiko, Opfer eines Cyberangriffs zu werden, stetig ansteigt. Daran ändert auch die Datenschutzgrundverordnung nichts – im Gegenteil. Umso wichtiger ist es also, dass Sie sich entsprechend vorbereiten und alle Anforderungen der DSGVO erfüllen, um auf der sicheren Seite zu sein. Das bedeutet vor allem eines: viel Arbeit. Doch worauf müssen Sie bei der Umsetzung tatsächlich achten? Und welche Punkte sollten Sie auf Ihrer DSGVO-Checkliste auf jeden Fall abgehakt haben?

4.2 DSGVO-Checkliste im Überblick

Was ist zu tun?	✔
Verantwortungsbereich klären – wer ist zuständig für die Umsetzung der DSGVO?	☐
Geschäftsleitung umfassend über Forderungen und mögliche Sanktionen bei Nicht-Umsetzung der DSGVO (z.B. 72-Stunden-Meldepflichten bei Sicherheitsvorfällen, Bußgelder, Imageverlust bei Datenpannen, etc.) informieren.	☐
Budget anpassen: Mögliche Kosten eines mangelhaften Datenschutzes bewerten und abwägen.	☐
IT-Struktur ermitteln und dokumentieren – mobile Endgeräte inbegriffen.	☐
Datenstruktur ermitteln und dokumentieren: Verschaffen Sie sich zeitnah einen Überblick darüber, wo sich welche Kundendaten befinden.	☐
Löschkonzept erarbeiten: Das Recht auf Vergessen umsetzen.	☐
Mögliche Datenübertragungen mittels Schnittstellen und gängigen maschinenlesbaren Formaten vorbereiten, um das Recht auf Datenübertragbarkeit von einem Anbieter auf einen anderen umsetzen zu können.	☐
IT belastbar und widerstandsfähig gegen Systemausfälle und Cyberangriffe aufstellen, um die Sicherheit der Datenverarbeitung nach DSGVO zu erzielen.	☐
Verschlüsselung der Daten verbessern.	☐
Datenschutzmaßnahmen ergreifen und deren Umsetzung dokumentieren sowie kontrollieren. Wenn es zu einer Prüfung kommt, möchten die Aufsichtsbehörden genau das sehen.	☐
Technischer Datenschutz: Sind die Maßnahmen dem Risiko entsprechend angemessen und entsprechen dem Stand der Technik?	☐
Aufsichtsbehörde kontaktieren und Beratung und Unterstützung suchen. Die Aufsichtsbehörden kennen die Herausforderungen der DSGVO.	☐
Wirksamkeit evaluieren und interne Kontrollprozesse technischer & organisatorischer Prozesse einrichten. Die DSGVO sieht eine regelmäßige Überprüfung und Anpassung der Maßnahmen vor.	☐
Verarbeitungsverzeichnis: Ist es erstellt und aktuell?	☐
Auftragsverarbeitung: Haben Sie die Verträge angepasst?	☐
Haben Sie einen Datenschutzbeauftragten bestellt?	☐

5. IT-Sicherheit: Trends und neue Bedrohungen

Vor allem in den letzten Jahren hat die Anzahl großflächiger Cyberangriffe und Mega-Datenpannen enorm zugenommen. WannaCry und Petya sind dabei nur zwei der Cyberangriffe, die besonders im Gedächtnis geblieben sind. Doch die nächsten Attacken stehen schon in den Startlöchern. Cybersicherheit wird darum für Unternehmen nicht nur immer mehr zur Priorität, sondern auch immer mehr zur Herausforderung.

Da unser tägliches Leben vermehrt durch Vernetzung bestimmt ist – etwa beim Smart Home – liegen hier die größten Bedrohungen. Doch auch in der Industrie gibt es dank Automatisierung und neuen Technologien immer mehr Sicherheitslücken, die sich nur schwer stopfen lassen und Hackern Tür und Tor für einen Angriff öffnen. Das größte Problem dabei ist, dass sich die Angriffe immer mehr wandeln. Sie werden nicht nur gezielter ausgeführt, sondern finden auch immer neue Angriffsziele – etwa im Industrie-, Gesundheits- oder Energiesektor. Doch welche Trends gibt es aktuell in puncto IT-Sicherheit?

Cybersicherheits-Trends

- *Datenschutz*
- *Internet of Things (IoT)*
- *Industrial Internet*
- *Neue Konzepte, um Bedrohungen zu erkennen*
- *Künstliche Intelligenz*
- *Zertifizierungen*
- *Biometrische Authentifizierung*
- *Neue Angriffsziele, z. B. im Gesundheits- / Energiesektor*

Alte Masche, neue Bedrohung – so ändern sich typische Angriffspunkte:

Bereits zu Beginn dieses Whitepapers haben wir einen Blick auf die größten Bedrohungen für die IT-Sicherheit geworfen. An den einzelnen Angriffspunkten hat sich in den letzten Jahren nur wenig geändert: Phishing und Datenklau sind auch heute noch die beliebtesten und effektivsten Angriffsmethoden für Hacker. Doch die Angriffsweise hat sich seither deutlich gewandelt: Es kommen immer neue Technologien zum Einsatz.

27% der Unternehmen glauben, dass Cyberangriffe häufig unbemerkt bleiben.

Auch Ransomware ist weiterhin eine große Gefahr, denn hier finden die Angreifer ebenfalls neue Möglichkeiten, Dateien zu verschlüsseln und Unternehmen damit zu erpressen. Außerdem nehmen Cyberkriminelle bei Ransomware-Angriffen vermehrt einzelne Unternehmen gezielt ins Visier, statt wie bisher auf groß angelegte Lösegeldforderungen zu setzen.

Für Unternehmen bedeutet das daher, noch mehr in die IT-Sicherheit zu investieren. Immerhin: Das Bewusstsein, wie wichtig IT-Sicherheit wirklich ist, ist bei den meisten Unternehmen gegeben. In einer Studie des Softwareunternehmens Kaseya aus dem Juli 2018* gaben 54 Prozent der Befragten an, dass IT-Security im Jahr 2018 ihr Hauptanliegen sei. Mit Blick auf das Jahr 2019 glauben sogar knapp 60 Prozent, dass IT-Sicherheit ganz oben auf der Prioritätenliste landen wird.

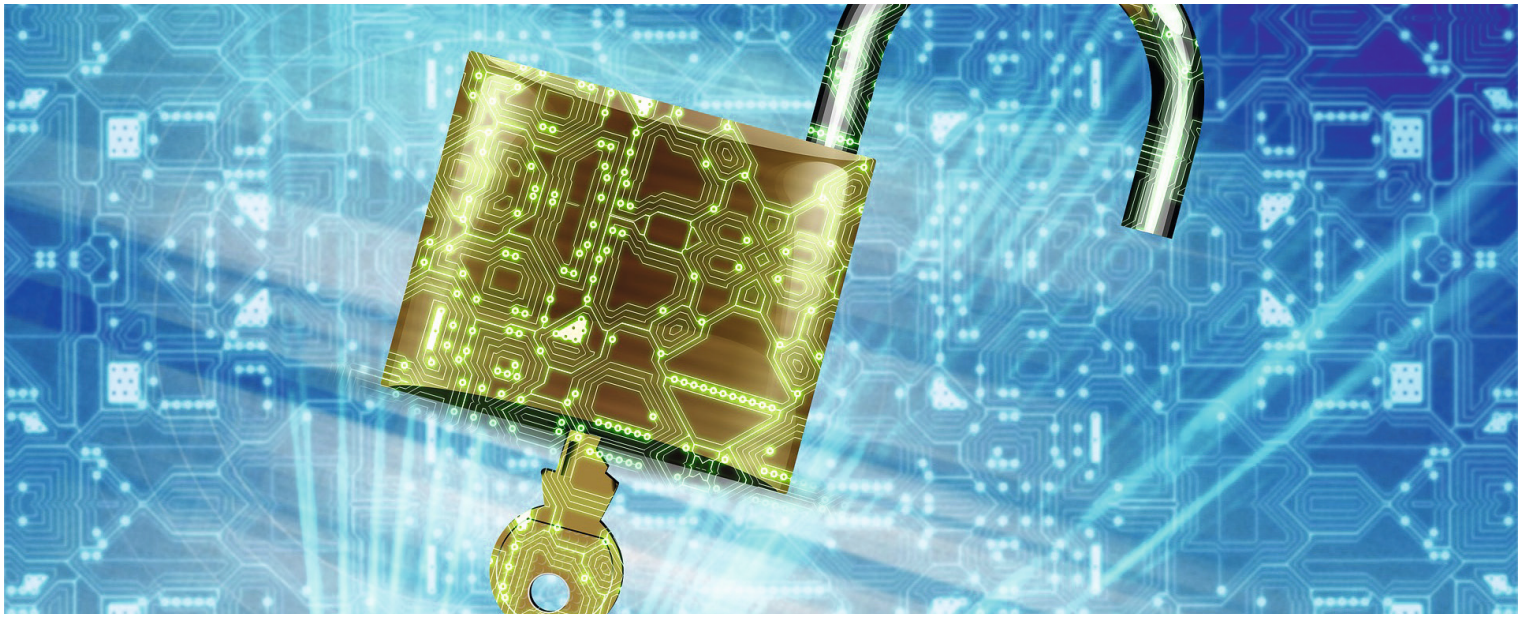
** Quelle: Kaseya: www.kaseya.com/resource/2018-state-of-it-operations-for-midsize-enterprises*

Ihr IT-Sicherheits-Schnellcheck

	Wissen Sie, ob Ihr Unternehmen ausreichend abgesichert ist?	Ja	Nein	k. A.
1.	*Kennen Sie jede aktuell eingesetzte Software auf allen Rechnern in Ihrem Unternehmen?*			
2.	*Sind Sie sicher, dass Ihre PCs tagesaktuell mit Sicherheitsupdates versorgt werden?*			
3.	*Setzen Sie ein Virenschutzprogramm und eine Firewall ein und aktualisieren Sie diese regelmäßig?*			
4.	*Haben Sie eine Datensicherung eingerichtet?*			
5.	*Sind Ihre Mitarbeiter zu den Themen Phishing, Spam und Social Engineering geschult und ist die Schulung aktuell?*			
6.	*Werden Ihre Betriebssysteme mit aktuellen Sicherheitsupdates versorgt?*			
7.	*Gibt es bei Ihnen ein Rechtemanagement, das sicherstellt, dass nur Mitarbeiter Administratorrechte besitzen, die diese zwingend benötigen?*			
8.	*Haben Sie alle Vorgaben zur DSGVO in Ihrem Unternehmen umgesetzt?*			
9.	*Haben Sie einen Notfallplan im Falle eines Cyberangriffs oder einer Datenpanne?*			

Sie können nicht jede Frage mit einem »Ja« beantworten oder erkennen direkt Handlungsbedarf? Dann wenden Sie sich an uns.

Wir kümmern uns um Ihre IT-Sicherheit und helfen Ihnen dabei, Ihre IT-Infrastruktur optimal zu schützen.



ToasterNET

Impressum

ToasterNet GmbH
Bahnhofplatz 1 | 91054 Erlangen
Telefon: +49 9131 91894730 | Fax: +49 9131 91894739
info@toasternet.eu
http://www.toasternet.eu