GBS

Expertise matters

Schluss mit Cyberattacken!

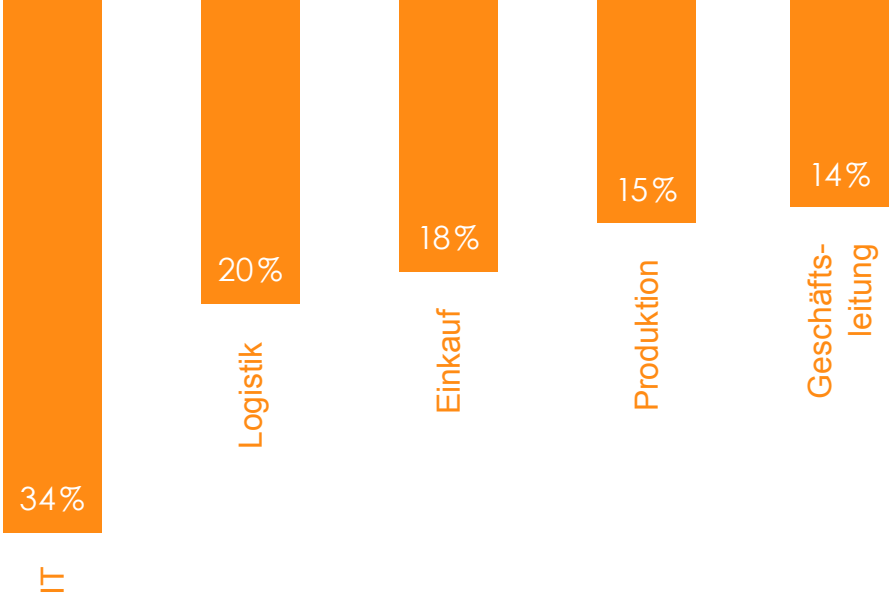
Die Top 10 Tipps für mehr Sicherheit

Cyberattacken auf dem **Vormarsch** »

Die Vernetzung aller Geschäfts- und Lebensbereiche nimmt massiv zu. Immer mehr Geschäftsprozesse finden online statt und mit jedem Klick wächst der Datenberg.
Ein Beispiel: Schon heute werden etwa 205 Milliarden E-Mails weltweit jeden Tag versendet und empfangen. Die Hälfte davon, 109 Milliarden sind geschäftlicher Natur – mit hochsensiblen und vertraulichen Inhalten. 2019 sollen es schon über 236 Milliarden E-Mails insgesamt sein. Davon gehen die Marktforscher der Radicati Group aus. »

» Angesichts solcher Zahlen muss das Bewusstsein jedes Einzelnen für einen verantwortungsvollen Umgang mit Daten geschärft werden. Gefragt sind auch Technologien, die den Datenschutz wahren. Denn die Computerkriminalität in der deutschen Wirtschaft wächst. Immerhin sind sich CIOs der Bedrohungslage durch Cybercrime und Wirtschaftsspionage bewusst: IT-Sicherheit ist neben Big Data eines der wichtigsten Themen dieses Jahres. Für 61% aller Befragten einer Trendumfrage der Bitkom ist IT-Sicherheit sogar das Top-Thema 2015. Und zwar nicht ohne Grund: Unternehmen waren in den letzten Wochen und Monaten zahlreichen Cyberattacken, Datendiebstählen, Ausspäh- oder Abhöraffären ausgesetzt. So wundert es wenig, dass Cyberattacken längst zum Alltag deutscher Unternehmen gehören. Wie der BITKOM in einer Studie vom April 2015 bekannt gab, war jedes 2. Unternehmen in den vergangenen zwei Jahren von Datenklau, Wirtschaftsspionage oder Sabotage betroffen. Unternehmen aus Industrie, besonders Automobil-, Chemie- sowie Pharmaindustrie, und dem Finanzwesen traf es dabei am häufigsten. Das Medium E-Mail wird dabei gern als potentielles Einfallstor verwendet. So ermittelte das Bundesamt für Sicherheit in der Informationstechnik (BSI) einen Anstieg von E-Mails mit Schadsoftware um 36% im vergangenen Jahr. »

Sicherheit geht uns alle an!



Angriffsziele

Quelle: Bitkom 2015

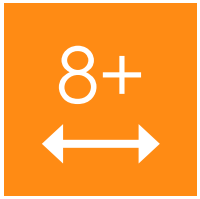
Stellt sich die Frage, was Unternehmen **konkret** gegen Cyberattacken machen können?

Gefragt ist eine Kombination aus organisatorischen und technischen Maßnahmen, die bei jedem Einzelnen greifen. Die wichtigsten Tipps auf dem Weg zu einer besseren Datensicherheit haben wir im Folgenden für Sie zusammengestellt!

Nur ein **starkes** Passwort, ist ein gutes Passwort »

Wie Sie es nicht machen sollten, zeigt eine Untersuchung von SplashData. Die Liste der 25 meist verwendeten und zugleich schlimmsten Passwörter wird angeführt von „123456“, „passwort“ oder „qwerty“. Beliebt sind auch Kombinationen aus Vor-/Nachname oder Wohnort.

Daher unser Tipp:
Nutzen Sie Groß-/Kleinschreibung, Zahlen und Sonderzeichen. Oder prägen Sie sich einen Satz ein und verwenden Sie den ersten Buchstaben jeden Wortes als Passwort. Außerdem empfehlen wir die Verwendung individueller Passwörter für unterschiedliche Konten. Und vergessen Sie auch nicht bei Ihrem E-Mail-Konto das Passwort in regelmäßigen Abständen zu ändern. »



8+ Zeichen

GROSS/klein

Zahlen

Verfremdung

Keine Wörter

Das hat den Vorteil, dass wenn ein Account gehackt wird, nicht gleich alle Zugänge gefährdet sind. Jetzt könnten Sie einwenden, dass viele und zugleich komplexe Passwörter natürlich schwer zu merken sind. Doch auch hier gibt es Lösungen. Mit kleinen Softwaretools wie KeePass lässt sich die Passworterstellung und -verwaltung vereinfachen. KeePass sichert sämtliche Zugänge in einer verschlüsselten Datei und ermöglicht das automatisierte Eintragen von Zugangsdaten in die Anmeldemasken von Webseiten. Damit steht auch der Verwendung komplexer Passwörter nichts mehr im Weg!

Wie genau KeePass funktioniert erfahren Sie in unserem Blog.

Auf **Aktualität** kommt es an »

Verwenden Sie einen Viren- und Spamschutz? Dann werden schon große Teile an Malware, Viren und Spam abgefangen. Doch achten Sie darauf, dass dieser Schutz stets aktuell ist. Denn mittlerweile erscheinen neue Bedrohungen im Stundenrhythmus. Nur ein aktueller Schutz ist ein guter Schutz. Haben Sie also stets einen Blick auf den Aktualisierungsstatus Ihrer Sicherheitslösungen.

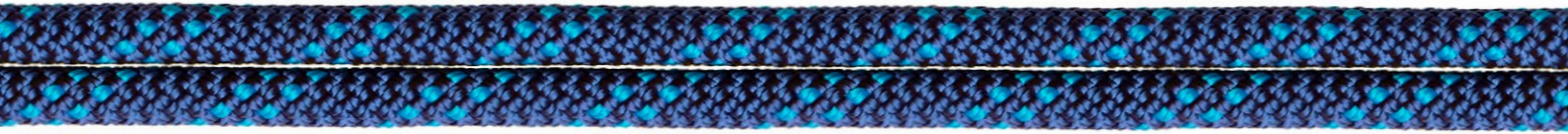
Rechtzeitig vorbeugen

Auch neue Cloud-basierte Erkennungstechnologien können helfen, sogenannte Zero-Day Exploits bzw. Attacken zu erkennen – also Angriffe, die gerade erst im Entstehen sind und bei denen klassische Muster-basierte Verfahren versagen würden.

Doppelt hält besser »

Schon längst gang und gäbe in Unternehmen: Mehrstufige Sicherheitsmechanismen, die beispielsweise vor Einbrechern schützen sollen. Dazu gehören im einfachsten Fall Schließ- und Zugangssysteme bis hin zur Videoüberwachung oder Bewegungsmeldern.

In der virtuellen Welt verhält es sich nicht anders. Legen Sie die Hürden höher, indem Sie mehrstufige Viren- und Spam-Abwehrmechanismen integrieren. Denn nicht immer ist gewährleistet, dass ein einzelner Anbieter wirklich alle Bedrohungen tagesaktuell erkennt. »



Nutzen Sie daher besser zwei Anti-Viren Technologien unterschiedlicher Hersteller.

Denn oft gilt: Was A nicht kennt, hat B womöglich schon integriert und kann die Bedrohung abwehren. Dieser zusätzliche Schutz belastet Budgets meist nur gering, bietet aber das entscheidende Mehr an Sicherheit für Ihre geschäftskritischen Daten!

Vier Augen sehen **mehr**
als zwei »

Der unerwünschte Abfluss von Daten und die damit einhergehende Abwehr, auch bekannt als Data Leakage Prevention, gewinnt zunehmend an Bedeutung in Unternehmen. Denn nicht immer sind es dreiste Datendiebe, welche von außen versuchen Ihr wertvolles Wissen abzugreifen. Oft sind es auch die eigenen Mitarbeiter, welche willentlich oder versehentlich zum Schlupfloch sensibler Daten werden. Gut gewappnet ist derjenige, der hier vorbeugt. Es gilt das alte Sprichwort: Vorbeugen ist besser (und billiger) als Nachsorgen. Schützen Sie also wichtige Daten vor Diebstahl. Ein intelligentes 4-Augen-Prinzip kann helfen. So lassen sich beispielsweise in der E-Mail-Kommunikation automatisierte Mechanismen integrieren, die einen Versand geschäftskritischer Daten verhindern. Seien es bestimmte Dateiformate, wie Excel-Dateien, welche Kundenlisten enthalten könnten oder bestimmte Textformate, die Kreditkartennummern ähneln – all das lässt sich erkennen und vor dem Versand blockieren.

Oft übersehen: Schutz der ausgehenden Kommunikation

Erst nach einer eingehenden 4-Augen-Prüfung durch eine zweite Person kann dann der Versand final freigegeben werden. Dieser eine Arbeitsschritt kann oft über Wohl und Wehe eines Unternehmens entscheiden. Denn ein Datenklau bringt nicht nur unvorhersehbare finanzielle Schäden mit sich, sondern hat meist auch langfristige Schäden für das Image eines Unternehmens zur Folge.

Verschlüsseln will gelernt sein »

Dass Daten abgefangen werden, ist nicht mehr die Ausnahme, sondern die traurige Regel. Gerade im Bereich der elektronischen Kommunikation sind sogenannte Man-in-the-Middle Attacken beliebte Angriffsszenarien, um an vertrauliche Inhalte zu gelangen. Stellt sich die Frage, warum viele Unternehmen nur unzureichend geschützt sind. Denn hier hilft nur eines: Verschlüsselung. Dabei sind im Wesentlichen zwei Arten zu unterscheiden.

Balance zwischen Sicherheit & Bedienbarkeit sicherstellen

Zum einen die Verschlüsselung des Transportweges. Hier kommt beispielsweise das https-Protokoll in Frage. Moderne Sicherheitslösungen haben dies in ihre Architektur oftmals integriert. Eine weitere Variante ist die eigentliche Verschlüsselung der zu übertragenden Daten. Im E-Mail-Bereich gibt es dazu bewährte Verfahren, wie beispielsweise S/MIME oder PGP. Oft scheuen Unternehmen jedoch deren Einsatz. Aufgrund der zugrundeliegenden Kom- »

Was bedeutet eigentlich S/MIME und PGP

S/MIME und PGP sind hochsichere Standards zum Verschlüsseln und Signieren von E-Mails.

Die Verschlüsselung erfolgt mit Hilfe eines öffentlichen Schlüssels, der zwischen den Kommunikationspartnern ausgetauscht wird und die Entschlüsselung durch den privaten Schlüssel des Empfängers, der auch nur diesem vorliegt. Die Signatur dient zur Bestätigung der Echtheit des Absenders und um zu überprüfen, ob der Inhalt der Nachricht noch nachträglich verändert wurde. Anders als bei PGP kommen bei S/MIME Zertifikate zum Einsatz, die von einer zentralen Zertifizierungsstelle ausgestellt werden.

plexität gibt es meist viele Schlüssel und Zertifikate zu verwalten. Diese Komplexität können Sie jedoch reduzieren, indem Sie auf zentrale, serverbasierte Lösungen setzen. Gegenüber Client-basierten Verfahren benötigen Sie hier viel weniger Schlüssel und Zertifikate. Der eigentliche Clou: Der Endanwender bekommt von der ganzen Ver- und Entschlüsselung nichts mit, da es zentral abläuft. Alternativ existieren neuartige Lösungen, die auf den Einsatz von Web-Technologien oder des PDF-Standards setzen. Hier benötigt der Empfänger keine spezielle Soft- oder Hardware zum Entschlüsseln der Inhalte. Sprechen Sie einfach Ihren Lösungspartner an.

Social ist **nicht**

immer gut »

Jeder kennt ihn: den kleinen gelben Zettel, auch bekannt als Post-It. Doch sollten Sie sich davor hüten, Passwörter und Zugangsdaten darauf zu notieren und öffentlich sichtbar zu hinterlassen. Der Social-Faktor, also das Risiko, welches durch das Miteinander entsteht, ist nicht zu unterschätzen. Dass dies häufig der Fall ist, zeigt ein Gang durch Büroräume. Hier kleben solche Zettel mit Daten meist am Monitor. Das ist ein gefundenes Fressen für potentielle Datendiebe. Und nicht immer muss es der Kollege sein. Wenn Sie externe Besucher im Unternehmen haben, kann auch darin ein Risiko bestehen.

Besser absperren

Was auch gern vergessen wird, ist das Sperren des eigenen Rechners, wenn es zur Pause geht. Also denken Sie daran, dass das beste Passwort nichts nützt, wenn Sie Ihren Bildschirm beim Verlassen des Arbeitsplatzes nicht sperren!

Phishing for **compliments** »

Nein, hier geht es nicht um wohltuende Worte, sondern den Versuch an Ihre Daten zu gelangen. E-Mails, getarnt als seriöser Absender, werden nämlich immer professioneller. Amazon, PayPal & Co: Nicht immer ist drin, was drauf steht. Über so genannte Phishing-Mails, die täuschend echt wirken, versuchen Betrüger an Ihre vertraulichen Daten, bevorzugt an Ihre Bankverbindung, zu kommen. Sie erkennen Phishing E-Mails beispielsweise daran, dass Sie zu sofortigem Handeln auf- »

gefordert werden. Oder an Drohungen, einer unpersönliche Anrede oder der Abfrage Ihrer Passwörter, Kreditkartennummer, PIN oder TAN innerhalb eines Formulars der E-Mail. Phishing-Mails enthalten oft auch einen Link, der zu einer täuschend echt aussehenden Internetseite führt, beispielsweise der Ihrer Bank oder der eines Onlineshops. Sie werden dann aufgefordert, Ihre Daten unter Angabe Ihrer Bankverbindung „zu aktualisieren“. Geben Sie diese ein, macht der Angreifer fette Beute.

Auch hier gilt also: Passen Sie auf und überlegen Sie: Haben Sie wirklich eine Geschäftsbeziehung zum Absender, weil Sie beispielsweise dort Kunde sind? Zeigt der Link in der Mail auf das wirklich richtige Portal (Blick ins Impressum und Browser-Leiste werfen)? Sind Rechtschreibfehler im Text?

Übrigens

Banken werden Sie niemals per E-Mail auffordern, Ihre PIN preiszugeben oder sie online zu aktualisieren. Und auch die seriösen Online-Portale und Shops fragen üblicherweise die vertrauliche Passwortdaten direkt nach Anmeldung in ihrem Portal ab. Werden diese Daten zwischendurch abgefragt, handelt es sich höchstwahrscheinlich um einen Betrugsversuch.


Ein Klick will
gut **überlegt** sein »

Per E-Mail werden Anhänge aller Art versendet. Doch Vorsicht: Klicken Sie nicht wild drauflos – schon gar nicht, wenn Sie den Absender der E-Mail nicht kennen. E-Mails sind beliebte Träger von Schadsoftware. Oft werden Trojaner oder Viren als getarnte PDFs, ZIPs oder TXT-Dateien versendet. Stellen Sie also bitte sicher, dass die Quelle der E-Mail vertrauenswürdig ist. Am besten erkennen Sie dies, wenn der Absender eine digitale Signatur mitschickt. Ist keine digitale Signatur dabei, prüfen Sie, ob Sie etwas mit der Person oder Firma im Absender zu tun haben. Oftmals können Sie E-Mails mit Schadprogrammen im Anhang anhand einiger Indizien im E-Mail Text erkennen: Die Texte sind häufig schlampig und grob fehlerhaft geschrieben, meistens fehlen die persönliche Anrede und Grußformel. Sind Sie sich dennoch nicht sicher, fragen Sie Kollegen oder ziehen Sie die IT-Abteilung hinzu. Alternativ löschen Sie solche E-Mails samt Anhang.

Das Beruhigende

Sofern Sie den Dateianhang nicht geöffnet haben, ist auch ein mitgeschickter Virus oder Trojaner vom Rechner verschwunden. Moderne Lösungen zur Abwehr von Malware in E-Mails setzen zusätzlich auf sogenannte Fingerprints. Diese analysieren eindeutige Muster in Dateitypen und erkennen beispielsweise, wenn sich ein Virus im ausführbaren exe-Format als PDF-Datei tarnt.

Mobil und **sicher** zugleich »

Der Arbeitsplatz-PC ist gut gesichert. Doch die Absicherung der mobilen Geräte wird gern vergessen. Im Handumdrehen entsteht hier ein Einfallstor für Hacker und Datendiebe. Denn Smartphones und Tablet PCs sind immer öfter mit der Infrastruktur des Unternehmens verdrahtet. Und vom Mobilgerät in das interne Unternehmensnetz ist es dann nur noch ein kurzer Weg.

So könnten Diebe Ihr komplettes Adressbuch mit geschäftlichen Kontakten auslesen. Oder Ihren E-Mail-Verkehr mit Kunden auswerten und sensible Informationen erhalten.

Unser Tipp: Schützen Sie Ihr Mobilgerät mit einem Passwort. Nutzen Sie zusätzlich die Möglichkeiten zur Fernwartung bzw. Fernlöschung. »

Was bedeutet eigentlich MDM & BYOD

Unter MDM (= Mobile Device Management) versteht man die zentrale Verwaltung aller im Unternehmen eingesetzten Mobilgeräte. Hierbei wird neue Hardware in der Inventarliste aufgenommen, benötigte Firmenanwendungen installiert, der mobile Zugriff auf Unternehmensdaten gesteuert und der Schutz der auf dem Mobilgerät gespeicherten Daten sichergestellt.

Bei BYOD (= Bring your own Device) werden private Mobilgeräten zur geschäftlichen Arbeit eingesetzt und ins Unternehmensnetzwerk eingebunden. Als Teil des MDM müssen insbesondere private Daten und Unternehmensdaten voneinander getrennt und die Einhaltung des Datenschutzes gewährleistet werden.

Ob Apple iOS oder Google Android

Die mobilen Betriebssysteme bieten mittlerweile die Möglichkeit, gestohlene Geräte nicht nur aufzuspüren, sondern auch die Daten aus der Ferne zu löschen. Und sollten Sie über eine große Anzahl geschäftlich genutzter Geräte verfügen, denken Sie über den Einsatz einer Mobile Device Management (MDM) Software nach. Gerade in Zeiten von Bring-your-own-Device (BYOD) gewinnen solche Lösungen an Bedeutung.


Machen Sie
sich **schlau** »

Ohne ein grundlegendes Verständnis für das Thema IT-Sicherheit ist heute ein ausreichender Schutz sensibler Daten nicht möglich. Machen Sie Ihre Mitarbeiter deshalb auf die Gefahren aufmerksam: per Rundmail, im Internet, über Ihr Collaboration-System oder ganz klassisch über einen Aushang am schwarzen Brett. Bieten Sie beispielsweise regelmäßig kurze Schulungen zur aktuellen Bedrohungslage an, welche genauso gut als Websession funktionieren. Geben Sie Sicherheitstipps und etablieren Sie Mindeststandards für die IT-Sicherheit. Denken Sie auch immer an die Zielgruppe: Der Außendienstmitarbeiter, der mit seinem Notebook unterwegs ist, braucht andere Informationen als der Entwickler im Büro.

Vorbeugen schützt

Legen Sie bei Neueinstellungen unbedingt einen Hinweis der Betriebsvereinbarung bei, welcher über Datenschutz im Allgemeinen und die konkreten Richtlinien im Betrieb, Passwortstärke, Änderungsfrequenz, physische Gerätesicherheit usw. informiert. Denn nur gut informierte Mitarbeiter können den alltäglichen Gefahren durch Cyberattacken trotzen.

Das **Fazit** »

Auch wenn die Intensität von Cyberangriffen fortlaufend zunimmt, sind Unternehmen dieser Bedrohung nicht schutzlos ausgeliefert. Organisatorische Vorgaben und ein gesunder Menschenverstand erschweren es den potentiellen Angreifern. Im Zusammenspiel mit zentralen IT-Sicherheitslösungen, welche es erlauben schnell auf die sich ändernden Bedrohungsszenarien zu reagieren, ergibt sich ein hohes Schutzniveau. Auf diese Weise wird der einzelne Mitarbeiter am Arbeitsplatz als Gefahrenquelle ausgeschlossen. Denn zentrale Mechanismen lassen sich nur schwer versehentlich oder vorsätzlich umgehen. Damit können Sie sicher sein, dass Ihre geschäftskritischen und vertraulichen Daten auch in Zukunft vor Cyberattacken geschützt sind!

Wie gut sind Sie **geschützt?** »

Wie hoch ist Ihr Schutzbedarf? Finden Sie es jetzt heraus!

Mit unserem Kurz-Check ermitteln Sie im Handumdrehen, welche Sicherheitsmaßnahmen Sie bereits umgesetzt haben und wo noch Handlungsbedarf besteht. Damit stellen Sie die Weichen, um Cyberattacken einen Riegel vorzuschieben!

Es existiert ein unternehmensweites IT-Sicherheitskonzept

Es werden komplexe Passwörter verwendet (Groß-/Kleinschreibung, Sonderzeichen etc.)

Für unterschiedliche Konten werden individuelle Passwörter vergeben

Passwörter werden in regelmäßigen Abständen geändert

Es wird ein aktueller Viren- und Spamschutz verwendet

Viren- und Spamschutz sind mehrstufig bzw. zweifach ausgelegt

Vertrauliche E-Mails werden verschlüsselt versendet

Mitarbeiter sind über Risiken von Phishing und bösartigen Dateianhängen aufgeklärt

Es ist sichergestellt, dass keine Geschäftsgeheimnisse via E-Mail versendet werden können

Mobilgeräte sind mit einem Passwort geschützt

Mobilgeräte sind in ein zentrales Sicherheitskonzept eingebunden (z.B. MDM)

In der Betriebsvereinbarung gibt es Sicherheits- bzw. Datenschutzhinweise

Mitarbeiter werden regelmäßig geschult oder auf Sicherheitsprobleme hingewiesen

Impressum »

Bildnachweis

Titelmotiv:

Bild #75727547 © Sergey Nivens Fotolia.com

Inhalt:

Bild #67864969 © James Thew Fotolia.com
Bild #43946632 © Zerbor Fotolia.com
Bild #29068437 © fancyfocus Fotolia.com
Bild #72798938 © apops Fotolia.com
Bild #55951039 © bloomua Fotolia.com
Bild #80220567 © Mr Doomits Fotolia.com
Bild #54756017 © contrastwerkstatt Fotolia.com

Herausgeber

GBS Software AG
Ottostraße 4
76227 Karlsruhe

Tel.: +49 721 4901-0
info@de.gbs.com
www.gbs.com

www.gbs.com