Security Guideline

für KMU´s
zum Schutz vor Cyber-Angriffen

arcade

Je stärker die Digitalisierung fortschreitet, je mehr sie die Geschäftsprozesse der Unternehmen durchdringt, desto grösser ist die Gefahr, dass **Unternehmen Opfer von Cyberattacken** werden.

Im DACH-Raum haben laut der im Juli und August 2020 vom Beratungsunternehmen techconsult durchgeführten Studie **66 Prozent** der befragten Unternehmen in den letzten zwölf Monaten **Opfer eines Cyberangriffs** erfahren.

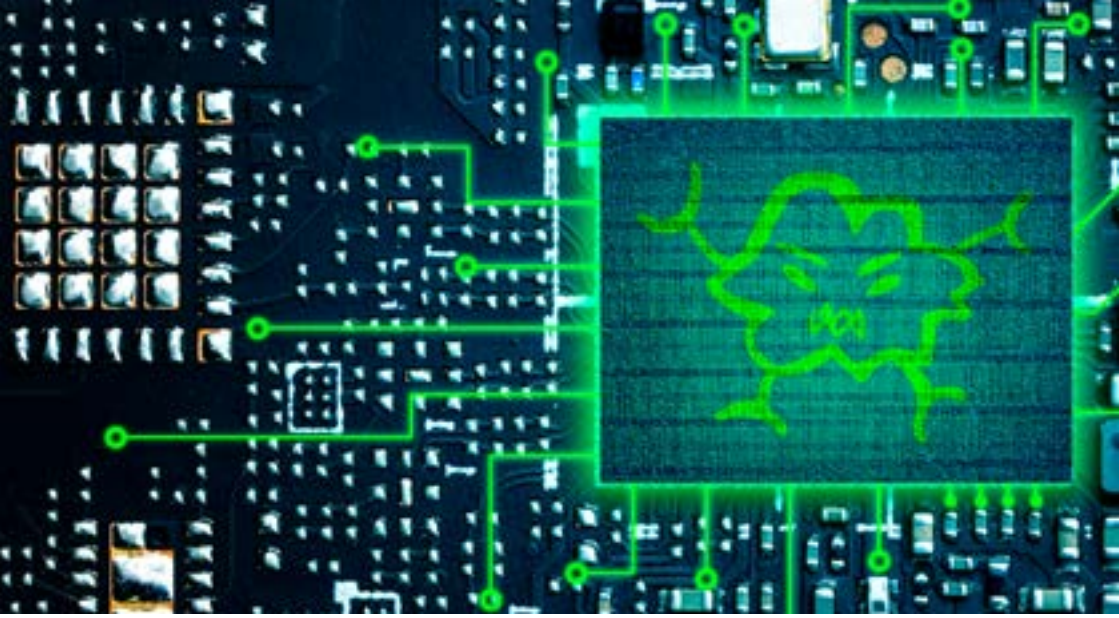
Laut Allianz Risk Barometer 2020 liegen **Cyber-Vorfälle** in der Schweiz auf Platz 1 der 10 **wichtigsten Geschäftsrisiken.** Zwar dürfte es jedem Geschäftsführer und Verwaltungsrat bewusst sein, dass es keinen 100%igen Schutz gegen Cyberangriffe gibt. Dennoch gibt es einige Punkte, die jedes Unternehmen in Sachen IT-Security mindestens erfüllen sollte, um sich möglichst gegen potenzielle **Cyber-Attacken zu schützen.**

Die folgenden sieben Handlungsempfehlungen fassen unsere Erkenntnisse von vergangenen IT-Sicherheitsrelevanten Ereignissen zusammen. Sie sollen dazu dienen, Ihr Unternehmen besser auf Cyberangriffe vorzubereiten und es vor kritischen Schäden zu bewahren.

1 Vorsichtiger Umgang mit öffentlichen Informationen.

Unternehmen sind heute gezwungen, im Internet präsent zu sein: Eine eigene Webseite, ein eigener Blog, ein Online-Shop, diverse Social-Media-Präsenzen usw. bieten Kunden, Lieferanten, aber auch anderen Personengruppen ein umfangreiches Bild des Unternehmens im Web.
Aber die Vernetzung geht noch weiter: Mitarbeiter besitzen berufliche Accounts bei LinkedIn und XING sowie private Accounts bei Facebook & Co. – jeweils gerne mit Verweis auf den Arbeitgeber. Sie melden sich mit der Firmen-E-Mail-Adresse für Newsletter an und tätigen Bestellungen im Namen ihres Arbeitgebers.
Alle diese Einträge, Präsenzen und Mitgliedschaften sind zusammen ein unfassbar grosser Pool an Daten – auch für Kriminelle. Wer diese Daten geschickt sammeln und auswerten kann, bekommt genügend Möglichkeiten für Cyberangriffe.
Studien belegen, dass sich Cyberkriminelle ihre Opfer viel gezielter aussuchen als vor wenigen Jahren. Sie planen ihre Angriffe von langer Hand und sammeln im Vorfeld wichtige Informationen – beispielsweise in den sozialen Netzwerken, oder direkt auf der Homepage Ihres Unternehmens. Darauf aufbauend passen sie ihre Angriffe entsprechend an, um einen legitimen Eindruck zu erwecken. Dies macht es für betroffene Mitarbeiter schwer, eine gefälschte von einer legitimen Nachricht (bspw. Phishing-Mail) zu unterscheiden und kann dazu führen, dass Mitarbeiter ungewollt zu Mittätern eines Cyberangriffs auf das eigene Unternehmen werden.

Unsere Empfehlung: *Unternehmen sollten stets genau abwägen, welche Daten und Informationen sie über welche Plattformen und Präsenzen preisgeben.*
Weiter sollen bindende Richtlinien definiert werden, wie sich die Mitarbeiter eines Unternehmens bezüglich ihrer Beziehung zum Unternehmen im Internet äussern dürfen.



2 Datensicherungskonzept mit Backup und Recovery-Strategie.

Cyberangriffe können verheerende Auswirkungen auf ein Unternehmen haben, welche bis zu dessen Konkurs reichen können[1], vor allem wenn Unternehmensdaten durch eine Ransomware verschlüsselt oder durch Viren gelöscht werden. Ein existenzbedrohender Schaden wird mitunter dann zur Realität, wenn keine aktuelle Datensicherung vorhanden ist. Das gleiche gilt auch, wenn Daten durch technische Fehlfunktionen, einen Brand oder absichtliches oder unabsichtliches Löschen von Mitarbeitern verloren gehen.

Für Unternehmen reicht es allerdings nicht aus, hin und wieder eine externe Festplatte an den Rechner anzuschliessen und ein Backup zu erstellen. Die Erfahrung zeigt, dass solche Backups in einem Ernstfall meist unvollständig oder sogar korrupt und somit unbrauchbar sind.
Daher ist es wichtig, ein angemessenes Datensicherungskonzept zu erstellen, mit dem genau festgelegt wird, wann welche Daten wie gesichert und aufbewahrt werden, wer die Passwörter für die verschlüsselte Wiederherstellung verwaltet und wer sich um die Backup- und Recovery-Software kümmert.

Unsere Empfehlung: *Erstellen Sie ein angemessenes Datensicherungskonzept. Sorgen Sie für eine passende Backup- und Recovery-Software, eine geeignete Aufbewahrung der Backup-Datenträger und regelmässige Wiederherstellungstests.*

[1] *https://www.srf.ch/news/regional/ostschweiz/konkurs-fensterhersteller-offenbar-zwang-eine-cyberattacke-swisswindows-in-die-knie*

3 Schutz sensibler Informationen durch professionelles Passwort-Management.

Wer sich unbefugt Zugriff auf einen fremden Rechner verschafft hat, gelangt neben dem Datenklau auf der lokalen Festplatte an die Passwörter für Programme, Cloudspeicher, Netzlaufwerke und Online-Dienste. Leider werden weitverbreitet nach wie vor diesselben Passwörter für mehrere Dienste verwendet. Dies führt dazu, dass bei einem Datenleck oft mehrere Services gleichzeitig kompromittiert werden.

Nebst dem ist auch die Passwort-Komplexität nach wie vor ein Problem. Man glaubt es kaum, aber die beliebtesten Passwörter des Jahres 2019 waren 123456 (Platz 1), 123456789 (Platz 2) und qwerty (Platz 3).[2] Auch der eigene Vorname oder das eigene Geburtsdatum sind sehr beliebt.
Abhilfe schaffen Sie mit einem professionellen Password-Manager, in welchem Sie Ihre Passwörter sicher erstellen, speichern und verwalten können.

Unsere Empfehlung: *Als Unternehmen sollten Sie eine Passwort-Management-Lösung einführen und allen Mitarbeitern zur Verfügung stellen. Durch die Verwendung einer solchen Lösung schaffen Sie für Angreifer eine weitere Hürde, zusätzliche Dienste erfolgreich zu attackieren.*

4 Doppelte Sicherheit beim Log-in.

Wie bereits erwähnt, sind schwache oder wiederverwendete Passwörter ein grosses Risiko für Unternehmen.
Sobald es Angreifern gelingt, einen Fuss in die Tür ihres Opfers zu setzen, beginnen sie, nach Privilegien und sensiblen Zugangsdaten Ausschau zu halten, die es ihnen ermöglichen, durch die Netzwerke zu bewegen und nach sensiblen Informationen zu suchen.

Um dieses Vorgehen zu verhindern hilft nur eine Lösung zur Multi-Faktor-Authentifizierung. Diese Art der Authentifizierung sichert Remote-Zugänge, Web-Applikationen, virtuelle Umgebungen und Cloud-Services durch eine starke Identitätsprüfung mit mehreren Faktoren wie Benutzername, Passwort und Einmal-PIN/Push-Benachrichtigung ab und stellt sicher, dass Angreifer auch dann keinen Zugriff auf Ihre IT-Systeme erhalten, wenn Passwörter abhanden gekommen sind.

Unsere Empfehlung: *Führen Sie in Ihrem Unternehmen zumindest für privilegierte Unternehmenskonten, Server, Cloud-Speicher und VPN-Tunnel die Multi-Faktor-Authentifizierung ein. Dies bietet einen optimalen Schutz der Unternehmensdaten und kritischen Applikationen.*

[2] *SplashData's Annual Worst Passwords List https://www.prweb.com/releases/what_do_password_and_president_trump_have_in_common_both_lost_ranking_on_splashdatas_annual_worst_passwords_list/prweb16794349.htm*

Heute kennen wir verschiedene Arten von Malware wie Viren, Würmer, Trojaner, Ransomware, Keylogger und Rootkits. Solche Schadprogramme verbreiten sich auf klassischen IT-Systemen zumeist über E-Mail-Anhänge, manipulierte Webseiten (Drive-by-Downloads) oder Datenträger. Der Hersteller Kaspersky entdeckt derzeit täglich 360.000 neue Schädlinge im Internet, Tendenz stark steigend.

5 Professioneller Schutz vor Schadprogrammen (Malware Protection).

Der Begriff Malware („malicious software“) wird häufig als Synonym für Begriffe wie Virus oder Trojaner verwendet. Tatsächlich ist Malware der Oberbegriff für eine Vielzahl an Bedrohungen, denen Anwender ausgesetzt sind. Heute kennen wir verschiedene Arten von Malware wie Viren, Würmer, Trojaner, Ransomware, Keylogger und Rootkits. Solche Schadprogramme verbreiten sich auf klassischen IT-Systemen zumeist über E-Mail-Anhänge, manipulierte Webseiten (Drive-by-Downloads) oder Datenträger. Professionelle Malware-Schutzprogramme sorgen heute nicht nur für die sichere Erkennung von bekannten Schadprogrammen, sondern können auch zuvor unbekannte Malware-Bedrohungen erkennen und davor warnen – basierend auf gemeinsamen technischen Merkmalen von Malware, wie z. B. dem Versuch, sich auf dem Computer zu verstecken.

Unsere Empfehlung: *Sparen Sie als Unternehmen nicht beim Malware-Schutz. Investieren Sie in eine professionelle Lösung für den Enterprise-Bereich mit auf Ihr Unternehmen zugeschnittenen Service- und Supportleistungen.*

6 Patchmanagement gegen Softwareschwachstellen.

Ein beliebtes Einfalltor sind veraltete Betriebssysteme, Software-Versionen und Apps. Die Hersteller und Entwickler sind stets bemüht, so schnell wie möglich Patches und Updates für entdeckte Lücken bereitzustellen. Nur müssen diese Patches und Updates vom Admin oder Nutzer auch installiert werden. Und hier liegt das Problem, denn die Update-Trägheit vieler Nutzer wird den Unternehmen immer öfter zum Verhängnis. Klar ist, dass die Verantwortung zum Aufspielen neuer Patchs nicht in den Händen der Nutzer liegen darf. Zeitmangel, fehlendes Bewusstsein für die Wichtigkeit von Patches oder einfach nur vergessen würde dazu führen, dass Sicherheitslücken eines Systems zu Sicherheitslücken für das gesamte Unternehmen werden. In Unternehmen, in denen viele Rechner und Softwareanwendungen im Einsatz sind, ist deshalb ein professionelles Patch- und Änderungsmanagements erforderlich. Dessen Aufgabe ist es, verändernde Eingriffe in Anwendungen, Infrastruktur, Dokumentationen, Prozessen und Verfahren steuer- und kontrollierbar zu gestalten.
Es müssen u. a. die Verantwortlichkeiten für Patches, die Ressourcen sowie die bestenfalls automatisierten Verteilungsroutinen von Patches und Änderungen definiert sein.[3]

Unsere Empfehlung: *Richten Sie ein professionelles Patch- und Änderungsmanagement ein, welches alle Verantwortlichkeiten und Ressourcen regelt. Patches und Änderungen müssen nach Wichtigkeit und Dringlichkeit klassifiziert, vor der Verbreitung getestet und anschliessend automatisiert ausgerollt werden.*

Professionelles Patch-Management ist essenziell, wie der Bericht des US-Computer Emergency Response Team zeigt. Denn für alle der Top 10 am meisten ausgenützten Schwachstellen würden Sicherheitsupdates zur Verfügung stehen.

[3] *https://us-cert.cisa.gov/ncas/alerts/aa20-133a*

7 Sensibilisierung der Mitarbeiter.

Die IT-Security-Experten sind sich darüber einig, dass den Mitarbeitern eine bedeutende, wenn nicht die bedeutendste Rolle bei der Abwehr von Cyberattacken zukommt. Denn technologische Schutzmassnahmen allein reichen nicht aus. Aufmerksame Mitarbeiter sind ein entscheidender Faktor bei der Abwehr von Cyberattacken.
Deshalb ist es wichtig, alle Mitarbeiterinnen und Mitarbeiter zu warnen, regelmässig zu informieren, zu schulen und zu sensibilisieren. Gerade, wenn diese

Unsere Empfehlung: *Bieten Sie in Ihrem Unternehmen regelmässig Schulung zum Thema IT-Sicherheit durch erfahrene Security-Experten an und machen Sie eine Teilnahme für alle Mitarbeiter verpflichtend.*

Kontakt im Notfall

Telefon	+41 41 417 31 70
E-Mail	support@arcade.ch
Stichwort:	**«kritischer Security Incident»**

arcade solutions ag • Winkelriedstrasse 37 • 6003 Luzern • +41 41 417 31 73 • arcade.ch

[4] *G DATA Mittelstandsreport 2019 https://www.gdata.de/news/g-data-studie-mitarbeiter-in-mittelstaendischen-unternehmen-loesen-cyberattacken-aus*