HISCOX

Tipps für mehr Cyber-Sicherheit

Checkliste & Glossar

In der heutigen digital vernetzten Welt ist Cyber-Sicherheit nicht mehr nur eine Option, sondern eine Notwendigkeit für Freelancer, Selbstständige und Unternehmen jeder Größe. Die Bedrohungen durch Cyber-Angriffe entwickeln sich ständig und in raschem Tempo weiter. Deshalb ist es wichtig ist, dass Sie sich und Ihr Business schützen. In dieser Checkliste bieten wir Ihnen **9 essenzielle Tipps**, um Ihre Cyber-Sicherheit zu stärken und die Risiken für Ihr Business zu minimieren.

Tipp: In unserem Glossar am Ende dieses Dokumentes haben wir für Sie Erläuterungen zu wichtigen Begriffen rund um das Thema Cyber-Sicherheit aufgenommen.

9 Tipps für Ihre Cyber-Sicherheit

1. Patchen (nachbessern) – und zwar regelmäßig

Eine Sicherheitslücke ist ein Softwarefehler oder eine Schwachstelle, durch den Kriminelle in Ihr Computersystem eindringen können. Eine Sicherheitslücke kann durch Programmierfehler im Betriebssystem, Internetbrowser oder anderen Softwareanwendungen entstehen. Um diese Lücken in ihren Programmen zu schließen oder Verbesserungen zu integrieren, bieten Hersteller sog. Patches (von Englisch „to patch“, übersetzt „flicken“) an. Meist werden Patches an regelmäßigen Patchdays eingeführt bzw. den Nutzern zur Verfügung gestellt. Für besonders kritische Sicherheitslücken gibt es außerdem Patches außerhalb der regelmäßigen Update-Rhythmen oder Anleitungen zur Behebung von Schwachstellen, sogenannte Fixes.

Unsere Tipps, um Sicherheitslücken zu vermeiden:

- ☐ Verfolgen Sie einschlägige Medien, um auf dem Laufenden zu bleiben
- ☐ Merken Sie sich Patchdays Ihrer Software-Anbieter im Kalender vor
- ☐ Führen Sie einen strukturierten Patchmanagement-Prozess ein
- ☐ Spielen Sie Sicherheitsupdates durchgehend und zeitnah ein

Denn wenn die Software (Firmware) auf dem neuesten Stand ist, sinkt das Risiko eines erfolgreichen Cyber-Angriffs signifikant.

2. Firewalls und Virenscanner verwenden

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) spricht von 250.000 neuen Varianten von Malware und 21.000 infizierten Systemen in Deutschland **pro Tag.** Die Segmentierung des Netzwerkes und das Nutzen von Firewalls und Virenscannern kann Ihr Risiko minimieren.

- ☐ **Virenscanner:** Achten Sie darauf, dass Sie einen tagesaktuellen Virenscanner nutzen. Denn der Virenscanner kann nur bei den Viren Alarm schlagen, die er auch kennt.
- ☐ **Firewall:** Die Firewall ist für Unternehmen besonders wichtig, da sie die Aufgabe hat, ein Netzwerk oder einen einzelnen Computer vor unerwünschtem Zugriff über Datenleitungen von außen, besonders über das Internet, zu schützen.

3. Sichere Passwörter und Multi-Faktor-Authentifizierung einrichten

Jedes Jahr führen Passwörter wie „123456“ oder „password“ die Listen mit den am häufigsten verwendeten Passwörtern an. Achten Sie daher auf **sichere Passwörter** und schützen Sie Ihre Zugänge über eine **Multi-Faktor-Authentifizierung.**
Für Unternehmen lohnt es sich, eine **Passwortrichtlinie** umzusetzen.

Ein sicheres Passwort sollte

- ☐ mindesten 8 Zeichen lang, dann aber komplex sein oder lang (ab 20 Zeichen) und etwas weniger komplex sein.
- ☐ Klein- und Großbuchstaben, Zahlen und Sonderzeichen enthalten.
- ☐ nicht im Wörterbuch vorkommen (auch nicht zwei zusammengesetzte Wörter).
- ☐ pro Account/System individuell festgelegt werden.

4. Zugriffsrechte einschränken

Richten Sie Beschränkungen für Zugriffsrechte für Benutzer ein, wenn Sie mit anderen arbeiten. Arbeiten Sie hier nach dem **Least-Privilege-Prinzip,** das jedem Nutzer nur die für ihn notwendigen Zugriffsrechte gewährt. Das betrifft auch die Absicherung von Fernzugriffen. Die Zugriffsrechte sollten zudem regelmäßig überprüft und aktualisiert werden.

Hier spielt auch die Netzwerksegmentierung eine wichtige Rolle. Welche Systeme müssen unbedingt miteinander verbunden sein und welche nicht? **Stellen Sie sich dabei Ihre IT-Sicherheit wie ein Schiff vor:** Sobald Wasser von außen in das Schiff

eindringt, können die Schotten niedergelassen werden. So läuft nur ein Bereich des Schiffes voll, die anderen aber nicht. Sind alle Systeme miteinander verbunden, haben Sie keine Schotten, die Sie herunterlassen können und der Angreifer hat vollen Zugang zu allen Systemen.

5. Sicherheitskopien erstellen

Cyber-Angriffe mit Erpressungssoftware (Ransomware) sind für Kriminelle ein einträgliches Geschäftsmodell. Wer seine Daten sichert, kann nicht so leicht erpresst werden. Erstellen Sie daher regelmäßig **Kopien (Backups) Ihrer Daten, auf die Kriminelle nicht zugreifen können.** Denken Sie hier wieder an das Schiff: Ihr Backup sollte in einem abgeschotteten Bereich liegen, in den das Wasser nicht laufen kann.

- ☐ Verwenden Sie für Ihr Backup ein **separiertes System mit separierter Nutzerverwaltung.** Stellen Sie sicher, dass in keiner Form direkt aus dem bestehenden System auf das Backup-System zugegriffen werden kann.
- ☐ Achten Sie bei **Cloud-Backups** (Auslagerung des Backups an einen Dritten) darauf, dass Sie Ihre Daten neben einem Passwort zusätzlich mit einem Token-Code oder einer PIN schützen. Denken Sie daran, die Zugangsdaten so aufzubewahren, dass Angreifer nicht darauf zugreifen können.
- ☐ Bewahren Sie Backups über **längere Zeit** auf, da sich Angreifer länger im System aufhalten können, bevor es zu einer Verschlüsselung der Daten kommt.
- ☐ Die Backups sollten **regelmäßig** auf Funktionalität, Konsistenz und Aktualität getestet werden.

6. Überwachungs- und Warnsysteme einrichten

Um zu erkennen, ob sich Angreifer im System befinden, sollten Sie für Ihr Unternehmen Tools nutzen, um den Zustand Ihres Systems zu überwachen und Abweichungen zu dokumentieren. Denn viele Angreifer bleiben zunächst „still“, um möglichst viele Daten abgreifen bzw. möglichst größten Schaden anrichten zu können. So erhalten Sie frühzeitig Hinweise auf verdächtiges Verhalten.

Außerdem:

- ☐ Verfolgen Sie auch Cyber-Sicherheitswarnungen einschlägiger Medien oder Einrichtungen, um auf dem Laufenden zu bleiben.
- ☐ Vergessen Sie nicht, Ihr IT-System zu dokumentieren. Dies hilft ungemein, falls es zum Schadenfall kommt und Ihr IT-System neu aufgebaut werden muss.

7. Ernstfall durchspielen

Um Ihre Prozesse optimieren zu können und im Ernstfall die Ruhe zu bewahren, lohnt es sich, den Krisenfall durchzuspielen und einen Krisenplan mit Ablaufplänen und Sofortmaßnahmen zu erstellen.

Stellen Sie sich dabei unter anderem folgende Fragen:

- ☐ Was könnte passieren und und welches sind die kritischen Systeme?
- ☐ Welche Netzwerke können kurzfristig getrennt werden, um eine Ausbreitung zu vermeiden?
- ☐ An wen können Sie sich für technische Hilfe wenden?
- ☐ An wen können Sie sich für juristische Hilfe wenden?
- ☐ Wen müssen Sie wann informieren?

8. Umgang mit Cyber-Risiken schulen

Längst haben Cyber-Kriminelle die „Schwachstelle Mensch“ in Sachen Cyber-Sicherheit erkannt. Eine große Rolle spielt hier **Social Engineering,** bei dem Angreifer das vermeintlich schwächste Glied in der Cyber-Sicherheitskette ins Visier nehmen. Beim Social Engineering werden menschliche Eigenschaften wie Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt, um Personen geschickt zu manipulieren. Zum Beispiel: **Phishing-Mails** mit schadhaften Links, auf die Sie klicken sollen – vermeintlich um beispielsweise Ihre Identität gegenüber Ihrer Bank zu bestätigen. Phishing-Mails sind gerade deshalb bei Kriminellen so beliebt, weil mit relativ wenig Aufwand, hoher Schaden angerichtet werden kann.

Daher ist es wichtig, dass Sie sich sowie Ihre Mitarbeitenden durch **regelmäßige Schulung im Umgang mit aktuellen IT-Sicherheitsthemen oder Angriffsmethoden** schulen. Behalten Sie dabei im Hinterkopf, dass Cyber-Kriminelle ihre Methoden ständig anpassen und weiterentwickeln – mitunter beschleunigt durch den inzwischen breiten Zugang zu Künstlicher Intelligenz.

9. Restrisiko absichern

Die genannten Tipps helfen Ihnen dabei, Ihre Cyber-Sicherheit zu stärken. Leider bedeuten allerdings selbst die besten Cyber-Schutzvorkehrungen nicht, dass ein Eindringen von Kriminellen in Ihr IT-System zu 100 Prozent verhindert werden kann. Denken Sie zurück an das Beispiel mit dem Schiff: Es ist wichtig, dass Sie an allen Stellen versuchen, Ihr Schiff vor dem Eintritt von Wasser zu schützen – ganz verhindern können Sie es aber nicht in jedem Fall. Daher sollten Sie sich für den Ernstfall absichern.

Eine **Cyber-Versicherung** hilft Ihnen, wenn es ein Angreifer in Ihr System geschafft hat – beispielsweise über einen infizierten Link in einer E-Mail. Hier ist es ratsam, auf einen Versicherer wie Hiscox mit **langfristiger Schadenerfahrung** zurückzugreifen, dessen Schaden-Service gut bewertet ist und der nicht zuletzt auch **umfangreiche Assistance-Leistungen** mit anbietet, also Sofort-Hilfe im Schadenfall z. B. in den Bereichen IT-Forensik, Datenschutz-Beratung oder Krisen-PR.

HISCOX

Ausgezeichneter Schadenservice
4,7 / 5
Kundenzufriedenheit (Kundenbefragung 2023)

Glossar: Wichtige Begriffe einfach erklärt

Backup	Eine Datensicherung oder Backup ist eine Kopie aller gespeicherten Daten mit dem Ziel, diese im Fall eines Datenverlustes (wie der Löschung oder Verschlüsselung) wiederherstellen zu können.
Compromised credentials	Indem persönliche Daten wie z.B. Passwörter gehackt und missbraucht werden, erlangen Cyber-Kriminelle unbefugte Zugriffe auf Konten, Systeme und Co.
Cyber-Risiken	Der Begriff „Cyber-Risiken“ bezeichnet Bedrohungen für Ihr Unternehmen, die durch moderne Informations- und Kommunikationstechnik wie Computer und das Internet entstehen. Im Fokus stehen Angriffe auf Ihre IT-Systeme oder Daten. Zum Beispiel: ■ Datenverluste und -missbrauch ■ Datenrechtsverletzungen ■ Datendiebstahl ■ Urheberrechtsverletzungen ■ Hackerangriffe ■ Betriebsunterbrechungen infolge von IT-Ausfällen
Cyber-Sicherheit	Cyber-Sicherheit umfasst den Schutz von digitaler Informations- und Kommunikationstechnik im Hinblick auf Vertraulichkeit, Verfügbarkeit oder Integrität. So dienen Cyber-Sicherheits-Maßnahmen dazu, Gefahren und Bedrohungen wie etwa Hackerangriffe oder Datenverlust und deren wirtschaftliche Schäden abzuwenden.
Denial-of-Service-Attacken	Ein DoS-Angriff beeinträchtigt IT-Systeme in Ihrem Unternehmen oder denen Ihrer Kunden maßgeblich. Sind gleich mehrere, miteinander vernetzte Computer davon betroffen, ist von einer DDoS-Attacke (destributed denial of service) die Rede. Übersetzt „Verweigerung des Dienstes“, sorgt ein DoS-Angriff mit massierten automatisierten Anfragen in kürzester Zeit dafür, dass der Server überlastet ist oder die Website ausfällt. Das kann große finanzielle Folgen für Sie haben, da weder Sie Zugriff auf Ihre Systeme haben noch Ihre Kunden Sie erreichen. Oder Ihr Kunde erleidet dadurch Umsatzausfälleund nimmt Sie für den entstandenen Schaden in Haftung.
IT-Sicherheit	Bei IT-Sicherheit bezieht man sich auf den Schutz von IT-Systemen vor Schäden und Bedrohungen. Dabei hat die IT-Sicherheit folgende drei Ziele: ■ Prävention von Angriffen ■ Das Erkennen von Angriffen ■ Reaktion auf Angriffe, um den Schaden so klein wie möglich zu halten
Phishing	Mit Phishing ist die illegale Methode gemeint, über gefälschte Webseiten, per E-Mail oder Kurznachrichten persönliche Daten oder Anmeldedaten von Internetnutzern abzugreifen. Die Daten eines Benutzers werden dann für betrügerische Aktionen genutzt.
Ransomware	Ein Angriff auf einen Computer oder ein System per schädlicher Software (Malware), die bösartig eingeschleust wurde. Die Malware sorgt dafür, dass der Computer infiziert wird und die Dateien auf der Festplatte und auf beschreibbaren Laufwerken verschlüsselt werden. Der Cyberkriminelle erpresst dann Lösegeld = Ransom, meist in Form digitaler Währungen dafür, dass dieser Vorgang von ihm rückgängig gemacht wird (Entschlüsselung).
Social Engineering	Der Begriff „Social Engineering“ bezeichnet eine Vorgehensweise, bei dem die Hilfsbereitschaft oder Gutgläubigkeit des „Faktor Mensch“ ausgenutzt wird. Zum Beispiel werden Mitarbeiter eines Unternehmens überzeugt, Sicherheitsvorkehrungen zu umgehen und sicherheitsrelevante Informationen preiszugeben.
Spear (targeted) Phishing	Eine besonders raffinierte Phishing-Variante, bei der Angreifer gezielt eine sehr persönlich zugeschnittene Ansprache nutzen, um Menschen zu verleiten, sensible Daten preiszugeben,
Zahlungsumleitungs-betrug	Beim Zahlungsumleitungsbetrug geben sich Kriminelle als Lieferanten/Geschäftspartner aus, sodass legitime Zahlungen auf die Konten der Betrüger geleitet werden.

Hiscox
Bernhard-Wicki-Straße 3, 80636 München