Was Sie über Cybersicherheit wissen müssen

- Die gefährlichsten Cyber-Bedrohungen
- Die Schwachpunkte, die Angreifer ausnutzen
- Wie Sie Ihr Unternehmen und Ihre Daten schützen

GlobalConnect

eGuide

Inhalt

GlobalConnect

„Neun von zehn Unternehmen von Datenklau, Spionage oder Sabotage betroffen.“

WirtschaftsWoche

“Hackerangriffe sind auf dem Vormarsch und kosten unsere Gesellschaft Milliardenbeträge. Es ist ein Wettrüsten.”

Claus Munch, Leiter der Backup-Services bei GlobalConnect Dänemark.

“Niemand kann sich da wegducken.”

Achim Berg, Bitkom.org

GlobalConnect

Cyberkriminalität ist ein echtes Geschäftsrisiko

Hackerangriffe kosten den deutschen Mittelstand 223 Milliarden Euro pro Jahr. „Neun von zehn Unternehmen sind von Datenklau, Spionage oder Sabotage betroffen“, schreibt die WirtschaftsWoche. Grundlage ist die aktuelle Studie[1] des Digitalverbandes Bitkom, von dem auch die anfangs erwähnte Zahl zum jährlichen Schaden stammt. Nahezu die komplette Wirtschaft sei in Deutschland von Cyberattacken betroffen, so der Bundesverband. „Niemand kann sich da wegducken“, sagte Bitkom-Präsident Achim Berg in Berlin gegenüber Tagesschau.de.

Vor allem im Mittelstand habe es deutliche Zuwächse gegeben. Die so verursachten Schäden haben sich im Vergleich zu den Vorjahren 2018/2019 mehr als vervierfacht. In Zukunft wird die Bedrohungslage durch Cyberattacken sogar noch ernster, so die in der deutschen Wirtschaft dominierende Meinung (83 Prozent der Befragten). Nicht nur das Geschäft mit der Cyberkriminalität boomt, auch die Bedrohung durch von Staaten engagierte Hacker wie aus Russland ist eine realistische Bedrohung, wie Experten im Handelsblatt[2] warnen. Diese könnten laut des Artikels als Antwort auf Sanktionen des Westens Angriffe starten.

Die Anzahl der Bedrohungen steigt mit der Wahrscheinlichkeit, selbst betroffen zu sein. Viele IT-Abteilungen sind heute beim Thema Sicherheit zwar aktiv, jedoch ist dabei die Hälfte der Technik inzwischen veraltet[3]. Hierbei spiele vorwiegend die Bezugsquelle eine große Rolle: Unternehmen mit Cloud-basierten Architekturen nehmen mehr als doppelt so häufig Aktualisierungen vor, als Firmen mit On-Premise-Technologien.

Zum Glück gibt es heute schnelle Abhilfe. Cloud-Technologie vereinfacht es die Unternehmensdaten abzusichern, das Geschäft zu schützen und Sicherheit im Alltag zu verbessern. Zudem bieten externe Dienstleister Sicherheitslösungen, die gegen DDoS und Ransomware-Angriffe schützen, sowie Backups wirkungsvoll absichern. So können sich Unternehmen wieder auf ihr Geschäft konzentrieren.

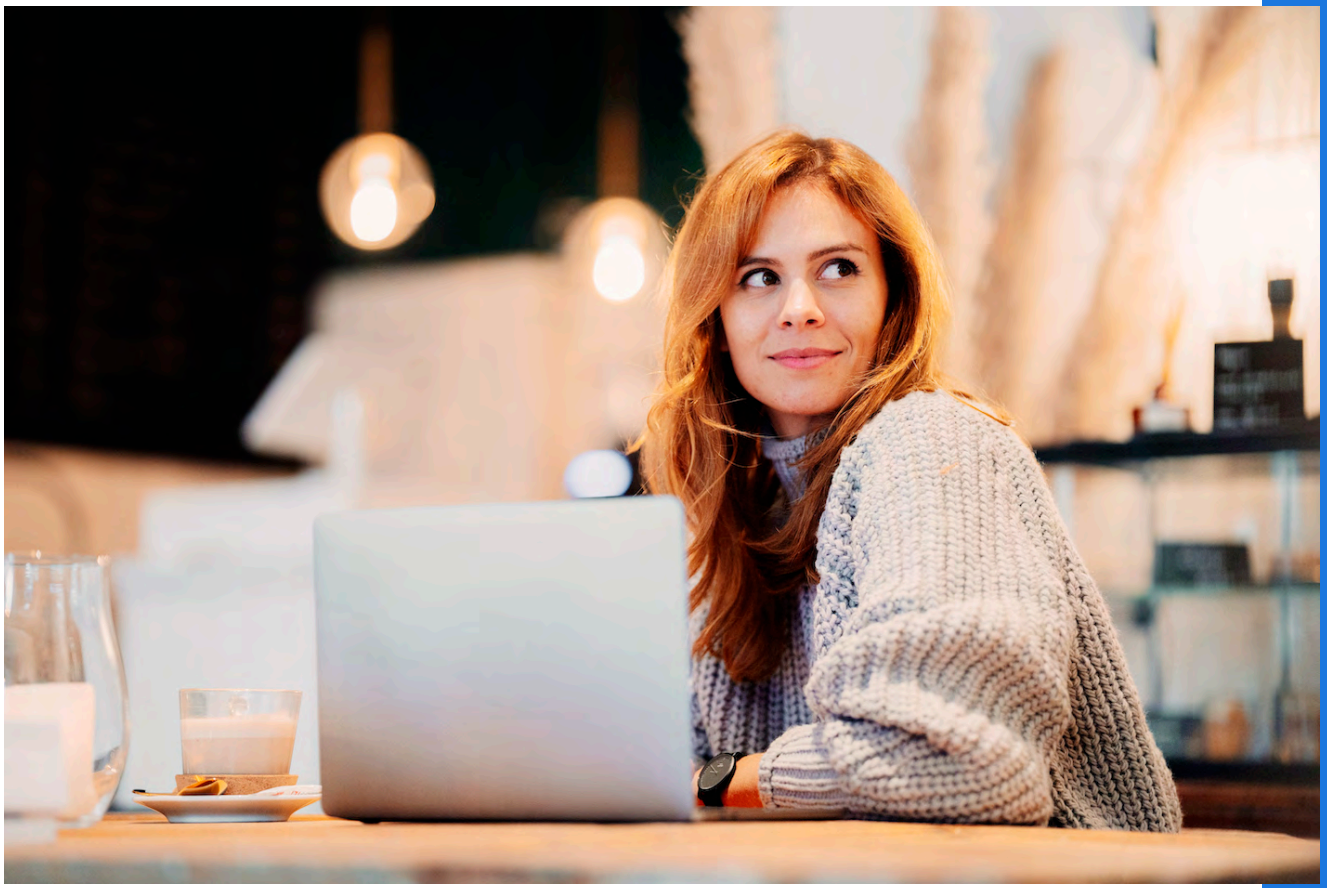
Wir haben diese Möglichkeiten für Sie kompakt in diesem Handbuch für Sie zusammengestellt

1 https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr
2 https://www.handelsblatt.com/technik/it-internet/ukraine-krieg-wir-sind-sehr-verwundbar-vier-gruende-warum-unternehmen-russische-hacker-fuerchten-sollten/28235336.html
3 https://blog.wiwo.de/look-at-it/2022/03/30/cybersecurity-2022-die-haelfte-der-deutschen-it-sicherheit-ist-veraltet/

Kennen Sie die gefährlichsten Cyber-Bedrohungen?

Cyberkriminelle erfinden ständig neue Wege, um Unternehmen und Organisationen anzugreifen.

Auf der nächsten Seite sehen Sie, welche Arten von Cyber-Angriffen derzeit am weitesten verbreitet sind. Diese sollten in Ihrer Cyber-Sicherheitsstrategie eine zentrale Rolle spielen.



- Ransomware
- DDoS
- Spoofing / Phishing
- Angriffe auf Backups

Ransomware: Lösegeld für Daten

Bei einer Attacke mit Ransomware wird ein Teil der Daten oder Systeme des Opfers verschlüsselt. Zuvor haben sich die Angreifer durch schadhafte Software (Malware) unbemerkt Zugang verschafft.

Für die Freigabe verlangen die Angreifer dann Lösegeld (englisch: ransom). 19 Prozent der gut 1.000 befragten deutschen Firmen erklärten in einer Studie von Bitkom, in den vergangenen zwölf Monaten von Ransomware angegriffen worden zu sein. Schäden durch Erpressung und Systemausfälle nennt die Studie Wirtschaftsschutz 2021 als mögliche Folgen.

DDoS: Existensbedrohende Ausfälle

DDoS („Distributed Denial of Service“)-Attacken überlasten den Server, von dessen Erreichbarkeit heute viele Unternehmen abhängig sind. Der Angreifer schickt gleichzeitig sehr viele Anfragen.

Die Website oder der Dienst wird in Folge mindestens stark eingebremst oder fällt aus. Kunden können die Website nicht mehr erreichen, es kommt zum „Denial of Service“.

Motivation und Ziele für die DDoS-Angriffe sind vielfältig. Sie reichen vom Geek- oder Hacker-„Sport“ (40 Prozent laut Bitkom) bis hin zu gezielten gelenkten Attacken. Diese können von Wettbewerbern, politischen Aktivisten oder organisierter Kriminalität stammen (Anstieg von 7 auf 29 Prozent in den letzten Jahren).

Spoofing/Phishing

Corona hat die Bedrohungslage noch einmal deutlich verschärft. Cyberkriminelle setzen gezielt auf Schwachpunkte. Der Faktor Mensch ist oft für die Angreifer eine Schwachstelle, ein beliebter Ansatzpunkt, um an Passwörter zu kommen. Und das ist nicht erst seit dem Homeoffice so.

Spoofing (englisch für Manipulation, Verschleierung) täuscht eine falsche Identität im Netzwerk vor. Bei Phishing zielen Angreifer darauf persönliche Daten wie Passwörter abzufangen. Beide Methoden hatten in Coronazeiten starken Zuwachs (12 Prozentpunkte) und sind heute immer noch eine beliebte Sicherheitslücke (siehe Seite 7).

Angriffe auf Backups: Der doppelte Boden ist weg

Backups sehen viele Unternehmen als Versicherung gegen Ransomware-Angriffe. Tatsächlich ist inzwischen die Datensicherung selbst oft Ziel von Angriffen. Hacker setzen wiederum Ransomware ein, um den Zugriff auf Ihren Computer und Ihre Daten zu blockieren.

Ein großer Teil des Problems besteht darin, dass heute alles online verfügbar ist. Sobald sich Unternehmen im Netzwerk befinden, können Hacker darauf zugreifen.

Beliebte Sicherheitslücken

Fragen Sie sich, warum Hacker und Cyberkriminelle immer noch relativ einfachen Zugang zu den Netzwerken vieler Unternehmen haben? Ist Cybersecurity nicht seit Jahren weltweit im Fokus? Werden Milliarden umsonst in Sicherheitslösungen investiert? Immer raffiniertere Methoden der Hacker sind nur ein Grund für den Boom der Cyberkriminalität. Tatsächlich ist oft das Verhalten der eigenen Mitarbeiter die größte Sicherheitsbedrohung.

Es hilft nichts, wenn ganz banale Sicherheitsregeln nicht eingehalten werden, etwa in Bezug auf Passwörter oder den physischen Zugang zu diversen Bereichen. Viele Unternehmen haben keine interne Sicherheitsrichtlinie formuliert. Und wenn doch, wird es den Mitarbeitern des Unternehmens nicht immer gut genug vermittelt.

Tatsächlich sind heute keine großen Anstrengungen für Hacker notwendig, um die IT-Infrastruktur des Unternehmens mit großen finanziellen Verlusten stillzulegen. Auf der nächsten Seite sehen Sie einige der beliebtesten Sicherheitslücken, die ungebetene Gäste oft verwenden, um sich in Ihr Netzwerk einzuschleichen.

Die Lieblings-Sicherheitslücken der Hacker:

- WLAN-Gastnetzwert
- Spam/E-Mails
- Netzwerkkabel
- IoT - Internet of Things

WLAN-Gästenetzwerk

Jeder möchte es seinen Gästen einfach und bequem machen. Aber wenn kein Zugangscode im Gastnetz vorhanden ist oder vielleicht nur ein einfacher (und damit schwacher) Code, sind Tür und Tor geöffnet: So kann sich ein Hacker von außen einloggen, zum Beispiel von einem unschuldig aussehenden Auto auf dem Parkplatz.

Nicht selten ist auch der Code für das Gastnetzwerk auf einem Schild sichtbar, das vom Fenster aus zu sehen ist. Und dann gibt es freien Zugang für unbefugte Gäste. Haben Sie übrigens sichergestellt, dass es nicht möglich ist, tief in das System und Netzwerk einzudringen, nur weil Sie als Gast im WLAN eingeloggt sind?

Netzwerkkabel

In den meisten Unternehmen gibt es über alle Netzwerkports vollen IP-Zugriff (das heißt, sie greifen auf das gesamte Netzwerk zu). Dies gilt häufig auch für Druckeranschlüsse.
Hier benötigen Hacker nicht einmal einen Code. Es reicht aus, sich physischen Zugang zu verschaffen, indem man sich beispielsweise als Handwerker oder vielleicht als Lieferant des täglichen Mittagessens ausgibt.

Dann muss der ungebetene Gast nur noch 20-30 Sekunden allein in einem Besprechungsraum oder im Druckerraum mit Netzwerkanschluss bleiben. Damit hat er hat freien Zugang.

Spam/E-Mails

Ein Klick auf einen Link oder das Herunterladen eines Anhangs von einem unbekannten oder maskierten Absender in einer betrügerischen E-Mail kann Hacker in hr Netzwerk einschleusen.

Vor ein paar Jahren waren solche E-Mails einfacher zu erkennen (etwa Nigeria-E-Mails in fehlerhaftem Englisch aus maschinellen Übersetzungen), aber heute erscheinen sie in Design und Sprache viel raffinierter und professioneller. Betrugs-E-Mails können heute wie eine Anfrage einer Behörde oder des CFO des Unternehmens aussehen, der schnell einige Anmeldeinformationen benötigt.

IoT - Internet of Things

Immer häufiger werden neuartige physikalische Geräte im Netzwerk eingesetzt, wie unter anderem Sprachassistenten, smarte Lichtsteuerung, Smart-TVs oder Produktionsmaschinen mit Internetanschluss.

Der Datenverkehr von diesen Geräten in (und aus!) Ihrem Netzwerk ist schwer zu überblicken. Viele der Geräte hören und tun viel mehr, als es in puncto Datensicherheit notwendig und angemessen ist. Daher sollten Sie sehr kritisch sein, was Sie mit dem Netzwerk verbinden. Überraschend viele Daten können zu und von Ihren IoT-Geräten fließen.

Investieren Sie jetzt in Sicherheit. Es zahlt sich aus.

Es ist nicht sinnvoll zu fragen, ob es sich lohnt, in professionelle und zeitgemäße Cybersicherheit zu investieren. Die bessere Frage ist: Können Sie es sich leisten, es nicht zu tun?

„Cyberangriffe sind zu einer enormen Bedrohung für die deutsche Wirtschaft geworden. Jedes zehnte Unternehmen sieht deshalb laut unseren Erkenntnissen seine Existenz bedroht. Der diesjährige Lagebericht des Bundesamtes für Sicherheit in der Informationstechnik untermauert eindrucksvoll, wie ernst die Lage für die deutsche Wirtschaft, aber auch für Privatpersonen, Behörden und andere Institutionen ist“, sagt Susanne Dehmel, Geschäftsleitung von Bitkom.org. Die Schäden durch Erpressung sind laut der Bitkom-Studie zur IT-Sicherheit von 2021 in den letzten drei Jahren um 358 Prozent gestiegen. Sie sind oft mit dem Ausfall von Systemen oder der Störung von Betriebsabläufen verbunden.

Die Investition in Sicherheitslösungen entspricht dem Abschluss einer anderen Versicherung, die Sicherheit im gesamten Unternehmen schafft. Wer würde zum Beispiel keine Haftpflicht- oder Einbruchsversicherung haben? Niemand. Sicherheitslösungen verhindern Cyberkriminalität. Sie sichern geschäftskritische Daten, die auch aufgrund von Umweltkatastrophen oder menschlichem Versagen verloren gehen können.

Neben den finanziellen Verlusten können erfolgreiche Cyberangriffe und vergeudete Sicherheit Ihrem Ruf ernsthaft schaden. Vor allem, wenn Sie in einer Branche tätig sind, in der die Sicherheit von Daten und Informationen entscheidend für das Vertrauen von Kunden und Partnern in das Unternehmen ist.

Ob versehentliche Pannen, ärgerliche Fehler oder reine Cyberkriminalität, das Worst-Case-Szenario ist dasselbe: Das Unternehmen kann am Ende erliegen und vollständig schließen. Das trifft laut Bitkom heute auf jedes zehnte Unternehmen in Deutschland zu – während neun von zehn bedroht sind. Es geht also nicht mehr um das „ob“, sondern „wann“ es ein Unternehmen trifft.

“Der Diebstahl von geistigem Eigentum kann für die innovati-onsgetriebene deutsche Wirtschaft schwerwie-gende Konsequenzen haben. ”

GlobalConnect

Fünf Tipps für mehr Sicherheit im Alltag

1

Werden Sie Teil eines Sicherheitsnetzwerks

Die Zeiten, in denen eine Firewall und ein wenig selbst gemachte Integration ausreichten, sind vorbei. Heutzutage ist es praktisch unmöglich, sich allein vor immer ausgefeilteren Sicherheitsbedrohungen zu schützen. Professionelle Hilfe ist gefragt. Ihre Sicherheitslösung sollte mit globalen Cybersicherheitsanbietern verbunden sein, damit die gesamte Software automatisch aktualisiert und vor neuen Bedrohungen geschützt wird. Viele IT-Anbieter bieten vorgefertigte Sicherheitspakete an, die in eine Komplettlösung mit Internetzugang eingebunden werden können.

2

Behalten Sie im Auge, wer Zugriff hat

Schaffen Sie Regeln und Restriktionen, die auf gesundem Menschenverstand basieren. So gibt es klare Empfehlungen dafür, wer welche IT-Einheiten, wofür was im Netzwerk nutzen darf. Zum Beispiel, dass ein Laptop in der Buchhaltung nur von der Buchhaltung angeschlossen werden darf und fünf ausgewählte Programme verwenden. Auf diese Weise kann Ihr Sicherheitssystem sofort erkennen, wenn etwas Ungewöhnliches passiert - und schnell darauf reagieren

3

Teilen Sie Ihr Netzwerk in Sicherheitszonen ein

Teilen Sie Ihre physischen und virtuellen Netzwerke in verschiedene Sicherheitsstufen ein. Nicht jeder sollte auf alles zugreifen können. Sie sollten festlegen, welche Geräte und Benutzer Zugriff auf welche Server und Rechenzentren haben. Außerdem sollten Sie Kabel und Anschlussports sichern, damit nicht alles Zugriff auf das gesamte Netzwerk gewährt. Bei besonders sensiblen Bereichen sollte das Mitarbeiternetzwerk physisch von den Teilen des Netzwerks getrennt werden, die nichts mit ihrer täglichen Arbeit zu tun haben.

4

Nutzen Sie Zwei-Faktor-Authentifizierung bei der Anmeldung

Es gibt einen sehr guten Grund, die zweistufige Authentifizierung (z. B. MS Authenticator) als Teil der Sicherheitslösung einzusetzen: Es funktioniert!
Ein Schlüsselcode auf einem Smartphone oder einem anderen physischen Gerät in Kombination mit Zugangsdaten aus Benutzernamen und Passwort ist für Hacker deutlich schwieriger zu überwinden. Selbst wenn Sie es schaffen ein Passwort mit einem Bot zu knacken, können sie sich nur mit Bestätigung vom Nutzer Zugang zum Netzwerk verschaffen – ohne Verifizierung bleiben sie draußen.

5

Definieren Sie automatische Sicherheitsprozesse

Tritt ein Sicherheitsproblem im Unternehmensnetzwerk auf, ist die Reaktionsgeschwindigkeit entscheidend für den Schaden an Daten und Infrastruktur. Verschiedene Stufen der automatischen Warnungen und Reaktionen verhindern, dass das Netzwerk bei jeder Kleinigkeit herunterfährt. Gleichzeitig sollte es bei ernsthaften Bedrohungen schnell reagieren. Mit einem professionellen IT-Partner können Sie solche Sicherheitsprozesse definieren.

Jetzt absichern – mit unseren Sicherheitslösungen

Sich gegen Hacker schützen ist nicht leicht, denn als Unternehmen bedeutet es weit mehr als nur zu aktuellen Bedrohungen auf dem Laufenden zu bleiben. Mit einem Partner erhalten Sie den bestmöglichen Schutz.

Sprechen Sie mit uns über Lösungen und Upgrades, die Sie gegen DDoS, Ransomware und Angriffe auf ihre Backups absichern.

Unser Service kümmert sich um alles – und Ihr Tagesgeschäft kann weiterlaufen.

Hier Beratungstermin vereinbaren und Zukunft sichern!

Rufen Sie uns an unter 0800 589 5424 oder kontaktieren Sie uns

DDoS-Rundumschutz

Der DDoS-Rundumschutz von GlobalConnect ist eine einfache wie kostengünstige Lösung. Unser Service kümmert sich um alles – und Ihr Tagesgeschäft kann weiterlaufen, mit Fokus und ohne Ablenkung.

Schutz vor Ransomware mit Veeam Cloud Connect

Backup-Daten sind ein beliebtes Ziel für Ransomware-Angriffe geworden. Deshalb ist ein stärkerer Fokus auf die Sicherheit von Backup-Daten wichtig – sowohl On-Premises als auch in Ihrer Cloud Repository. Veeam nutzt die Best Practice-Strategie 3-2-1-Backup.

GlobalConnect