HELMSAUER

GRUPPE

CYBERNews

Exklusiv. Aktuell. Informativ.

Cyberkriminalität – So schützen Sie Ihr Unternehmen

Cyberangriffe auf Unternehmen sind mittlerweile eine alltägliche Bedrohung, die neben Imageschäden hohe Kosten für die Betroffenen verursachen können. Aktuelle Untersuchungen zeigen, dass die Zahl der Angriffe in den letzten 2 Jahren deutlich gestiegen ist. Bereits in 2019 war jedes zweite Unternehmen betroffen. Auch im ersten Halbjahr 2020 stiegen die Zahlen weiterhin um 67 % im Vergleich zum Vorjahr.

Aktuelle Entwicklung

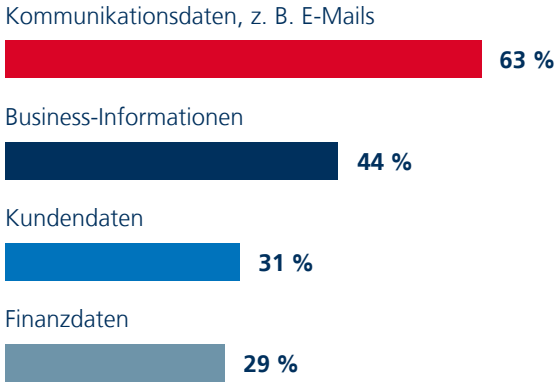
Die deutsche Wirtschaft ist mehr denn je von Cyberangriffen betroffen. Dadurch entstehen mittlerweile Schäden im Rekordwert von ca. 223 Milliarden Euro pro Jahr, was aus einer aktuellen Bitkom-Studie hervorgeht. „Niemand kann sich da wegducken", sagte Bitkom-Präsident Achim Berg. In den Jahren 2020 und 2021 waren fast 9 von 10 Unternehmen von Datenklau, Spionage oder Sabotage betroffen. Vor allem Erpressungen, verbunden mit dem Ausfall der Systeme oder Produktionsanlagen sowie Störungen in den Betriebsabläufen, erleben einen enormen Anstieg.

Cybercrime boomt durch Corona

Das vergangene Jahr war aufgrund der Coronapandemie voller Herausforderungen. Cyberkriminelle nutzten diese Krise schamlos aus. Neben einem rapiden Anstieg an Ransomware-Attacken, waren auch Social-Engineering-Maschen durch Coronabezug von Erfolg gekrönt. Cyberkriminelle haben bereits in den ersten Wochen der Pandemie coronaspezifische Inhalte in Phishing-Kampagnen einfließen lassen. Dies hat die durchschnittliche Klickrate von 29 % auf 78,8 % erhöht – nur durch das Wort „Corona" im Betreff. Neue Kommunikationswege und neue digitale Geschäftsprozesse halten nicht erst seit Covid-19 Einzug in das Geschäftsleben. Die Pandemie hat nur an vielen Stellen das Tempo erhöht. Experten gehen davon aus, dass das Homeoffice-Setting erfolgreiche Cyberangriffe wahrscheinlicher macht. Die Studie von SoSafe 2021 weist nach, dass die Klickrate auf Phishing-Mails in Homeoffices signifikant höher ist als in zentral aufgestellten Organisationen.

Kommunikationsdaten und geistiges Eigentum im Visier

In einer Studie von bitkom wurde 2021 veröffentlicht, welche Daten besonders in Unternehmen gestohlen worden sind.



Quelle: bitkom Research 2021

Praktische Beispiele – Schadenfälle in Unternehmen

Auftragsanfrage mit Folgen

Ein Unternehmen erhielt eine vermeintliche Auftragsanfrage per E-Mail. Die Mitarbeiterin im Büro öffnete diese zur Bearbeitung. Die Schadsoftware breitete sich unbemerkt im IT-System und damit in der Kundenverwaltung aus. Weder Firewall noch die Antivirussoftware griffen. Die Schadsoftware sendete heimlich Daten inkl. Bankverbindungen der Kunden an einen fremden Dritten.

Die Folgen sind …

+ Schadenermittlung (Forensik)
+ Säubern des Systems, Information der Betroffenen (geltendes Recht nach Bundesdatenschutzgesetz!)
+ PR- und Krisenmanagement
+ Wiederherstellung der Kundendatenbank
+ Schadensersatzforderungen von Kunden
+ Bußgelder ggf. Betriebsunterbrechung aufgrund Stilllegung der Systeme

Identitätsdiebstahl

Ein Unternehmen staunte nicht schlecht, als es bei der nächsten Rechnungsstellung für abgeschlossene Aufträge verwunderte und verärgerte Kunden am Telefon hatte, weshalb nun eine doppelte Abrechnung stattfinden würde. Nach weiterer Recherche stellte sich heraus, dass im Namen des Betriebes und optisch fast identisch, Rechnungen an Kunden gesendet worden sind, die diese auch umgehend beglichen hatten. Aufgrund der vorher engen Zusammenarbeit und der laufenden Aufträge über einen längeren Zeitraum waren die Kunden nicht misstrauisch geworden. Bei der Schadenermittlung stellte sich heraus, dass der Betrieb über Monate hinweg digital ausgespäht worden ist.

Die Folgen sind …

+ Schadenermittlung (Forensik)
+ Säubern des Systems
+ Wiederherstellung
+ Schadenersatzforderungen von Kunden
+ Information weiterer Betroffener

Wie das zweite Beispiel zeigt, gehört vor allem „Phishing“ zu den häufigsten Angriffsarten. Bei einem solchen Identitätsdiebstahl werden über gefälschte E-Mails Dritte dazu gebracht, Geldzahlungen zu leisten oder sensible Daten zu teilen. Diese Form des Betruges bedarf einer längeren Recherche, um an die erforderlichen Informationen des Betriebes zu gelangen. Regelmäßig erfolgt dies über Kompromittierung eines E-Mail-Accounts, Homepages oder direkte fingierte Anrufe im Betrieb. Deshalb ist es besonders wichtig zu erkennen, welche E-Mails vertrauenswürdig sind.

So schützen Sie sich aktiv

Die Untersuchungen haben gezeigt, dass viele erfolgreiche Cyberangriffe auf menschliches Handeln zurückzuführen sind. „Das größte Sicherheitsrisiko sitzt vor dem Bildschirm“, heißt es immer und das hat einen Vorteil. Welchen? Die Antwort lautet, dass dann Sicherheit und Schutz trainierbar sind. Über Sensibilisierung für Cybersicherheit, intelligente Sicherheitssoftware und schnelle Unterstützung von Experten im Ernstfall kann der Cyberangriff abgewehrt oder der Schaden gemindert werden. Durch die aktuellen Entwicklungen angeregt, bieten professionelle Dienstleister interessante Lösungen an:

Phishing-Tests

Um sich vor Phishing-Attacken zu schützen, müssen sie als solche erkannt werden. Dafür ist es notwendig, Ihr Wissen zu der Vorgehensweise und den Möglichkeiten der Kriminellen zu erweitern. Videobasierte, praxisorientierte Online-Trainings sowie Webinare, um zu lernen, wie jeder Laie solche E-Mails zu erkennen vermag, helfen immens. Die leicht verständlichen, kompakten und anwenderfreundlichen Einheiten sensibilisieren für das Risiko und sind einfach in den Alltag zu integrieren. Somit sind diese auch machbar, wenn wenig Zeit neben dem Beruf übrig bleibt. Dienstleister bieten zudem Phishing-Simulationen an. Sie und Ihre Mitarbeiter erhalten von dem Dienstleister über einen Zeitraum realitätsnahe Phishing-Emails und können so Ihr erlerntes Wissen als praktische Übung trainieren.

Intelligente Software

Moderne Sicherheitssoftware-Lösungen bieten nicht nur effektiven Antivirenschutz, sondern zusätzlichen Schutz über die Integration künstlicher Intelligenz und maschinelles Lernen. Dadurch wird die Schadsoftware nicht nur erkannt, sondern verhindert auch deren Installation. Viren, Trojaner, Würmer und andere Schadsoftware verändern sich schnell – oft täglich. Die künstliche Intelligenz datet sich live online up, lernt dazu und kann so gefährliche Ähnlichkeiten zu bekannter Schadsoftware erkennen. Dadurch wird ein deutlich umfangreicherer Schutz vor Cyberangriffen erreicht, als dies herkömmlich der Fall war.

Mitarbeiterschulungen –
online und jederzeit durchführbar

Schulungen sind dann am besten, wenn das Gelernte schnell im Alltag anwendbar ist. Kurze und kompakte Webinare informieren zu den Cyberrisiken im Betriebsalltag eines Unternehmens, sensibilisieren für die Thematik und liefern Unterstützung beim Schutz vor Cyberangriffen. In Kombination mit Online-Trainings für Mitarbeiter, die jederzeit durchführbar sind, werden die Abläufe im Betrieb nicht behindert. Dennoch lernen die Mitarbeiter gezielt und tragen so erheblich zur Sicherheit des Betriebes bei.

Werkzeugkasten – Hilfe für den Alltag

Mit gezielten Helfern für den Alltag sparen Sie Zeit und integrieren dennoch die notwendigen Maßnahmen zur Cybersicherheit in Ihren Betriebsalltag. Dienstleister bieten über ein Online-Portal, zu dem der Anwender einen individuellen und sicheren Zugang erhält, die technischen Helfer an. So lässt sich z. B. mit einem Klick der Browser auf den neuesten Stand überprüfen. Die neueste Software bietet immer die höchste Sicherheit. Passwort-Generatoren erstellen schnell und einfach sichere Passwörter. Mit E-Mail-Scans lassen sich binnen kurzer Zeit die eingehenden E-Mails auf gefährliche Inhalte überprüfen.

Hilfe im Notfall

Im Angriffsfall ist die schnelle und kompetente Hilfestellung von Profis ausschlaggebend für das Ausmaß der Schädigung. Cyberversicherungen decken nicht nur viele materielle Schäden, sondern bieten umfassende Serviceleistungen zur Schadenbekämpfung und aktiven Unterstützung im Ernstfall. Spezielle Produkte bieten den Zugriff auf Cybercrime-Dienstleister 24-Stunden, die Ihnen im Fall der Fälle rund um die Uhr schnelle Hilfe leisten und keine zusätzlichen Kosten anfallen.

Hilfe für den Ernstfall –
was ist bei einem aktiven Cyberangriff zu tun?

Im Falle eines akuten Cyberangriffes muss klar sein, wer was zu tun hat, welche Informationen benötigt werden und wie zu kommunizieren ist. Wie immer, wenn es um die Gestaltung von Prozessen geht, an denen mehrere Personen beteiligt sind, macht es Sinn, diese aufzuschreiben und für die Beteiligten jederzeit zugänglich zu machen. Aus diesem Grund ist es empfehlenswert, diese Abläufe in das Qualitätsmanagement des Unternehmens zu integrieren. Auch die Thematisierung in regelmäßigen Teambesprechungen schafft Nachhaltigkeit.

Notfall-Checkliste

- ✓ Foto vom Bildschirm mit Smartphone anfertigen (+ Protokoll, Datum, Uhrzeit)
- ✓ Alle Netzwerkverbindungen trennen
- ✓ Systemdokumente/-informationen griffbereit haben (Notfallplan)
- ✓ Professionellen Cybercrime-Experten kontaktieren
- ✓ Externen Zugang zu den Systemen zur Schadenfeststellung und Begrenzung ermöglichen
- ✓ Diskretion bewahren
- ✓ Kollegen anleiten A,B,C zu tun

Um im Ernstfall weitere Schäden zu vermeiden, sind korrekte Maßnahmen und schnelle Umsetzung entscheidend für das Ausmaß der Verwüstung. Die Unterbrechung der Internetverbindung und das Ausschalten der Geräte sind als Primärmaßnahme unerlässlich, um die Verbreitung im System möglichst einzuschränken. Meist lässt sich dies nicht mehr vollständig verhindern. Aus diesem Grund sind Profis gefragt. Auf die Abwehr von Cyberangriffe spezialisierte Dienstleister bieten einen Notfallsupport 24/7 und sind in der Lage, sich extern auf die Systeme zu schalten, eine erste Einschätzung der Situation zu geben und oftmals bereits mit der Bekämpfung zu beginnen. Der absolute Vorteil ist, dass sich diese Experten, im Vergleich zu herkömmlichen IT-Häusern, hauptberuflich mit der Abwehr von Cyberattacken beschäftigen. Dies führt zu dem Wissen, welche Schadsoftware aktuell in Umlauf ist und daraus eine schnelle Bekämpfung resultieren kann.

Das Ausmaß der Schädigung ist relevant für die daraus resultierenden Folgen. Diese gehen vorerst nur Sie etwas an! Interne und externe Diskretion ist unerlässlich, um möglicherweise Reputationsschäden zu vermeiden. So haben Sie noch die Chance, sich über die weiteren Schritte in Ruhe Gedanken zu machen und notfalls Beratung einzuholen. Zur Wahrung von Diskretion müssen Sie Ihr Personal anleiten. Zu empfehlen sind Checklisten im Rahmen des Qualitätsmanagements. Hier ein Beispiel zur Unterstützung im Ernstfall.

Wenn alle Stricke reißen

Sollte es trotz aller Vorsicht und Schutzmaßnahmen zu einem Cyberangriff kommen, ist es hilfreich, das Unternehmen über eine leistungsstarke **Cyberversicherung** abgesichert zu haben. Hier bieten wir ein spezielles Konzept, das besonders auf die Bedürfnisse von Unternehmen ausgelegt ist. Neben dem Versicherungsschutz erhalten Sie auch bereits einige der genannten Service-Leistungen und Schulungsprogramme kostenfrei. Aufgrund der aktuellen Entwicklungen ist es uns in diesem Jahr gelungen, die Inhalte des Rahmenkonzepts nochmals zu verbessern.

Rahmenkonzept für Sie nochmals verbessert:

- ✓ **Kostenfreies Cyber-Security-Training für alle!** Kostenfreier Zugang zu Online-Trainings und automatisierten Phishingtests sowie zahlreiche Schulungsvideos rund um das Thema Cybersicherheit für Sie und Ihre Mitarbeiter/-Innen. Zusätzlich kostenfreie Webinare zu aktuellen Entwicklungen der Cybercrime, Präventivmaßnahmen und Handlungsempfehlungen durch die Helmsauer Akademie
- ✓ **Zweifache Maximierung der Versicherungssumme**
- ✓ **Garantierte und unverzügliche Hilfestellung** im Schadenfall – Rund um die Uhr!
- ✓ **Mitversicherung von Eigenschäden** in der Forensik und Schadenfeststellung
- ✓ **Vermögensschäden aus gefälschten E-Mails** mit Aufforderung zu Geldtransaktionen
- ✓ **Wiederherstellungskosten** (inkl. Hardware-Ersatz)
- ✓ **Mitversicherung von Drittschäden**, z. B. Abwehr unberechtigter Schadenersatzansprüche
- ✓ Soweit gesetzlich zulässig: **Übernahme von Bußgeldern**
- ✓ **„Bring your own device"-Deckung** z. B. berufliche Nutzung privater Smartphones
- ✓ **Betriebsunterbrechung zur Sicherung Ihres Umsatzes** – Dies gilt auch bei technischen Störungen
- ✓ **Erweiterung** der Betriebsunterbrechungsleistung um Mehrkosten
- ✓ **Internet-Diebstahl**
- ✓ **Cyber-Spionage**
- ✓ **Cyber-Erpressung**

Ihre Hotline bei der Helmsauer Gruppe: **0911-9292 185**

> Rückantwortfax: 0911-9292 432

Ja, ich möchte weitere Informationen erhalten.
Bitte nehmen Sie mit mir Kontakt auf:

☐ Cyberversicherung ☐ Weiterbildungsangebot zur Cybersicherheit

☐ Herr ☐ Frau _____
Name, Vorname

_____ _____
E-Mail Telefon

Stempel:

ANTWORTSCHREIBEN an:

Helmsauer Gruppe
Dürrenhofstraße 4
90402 Nürnberg

Per E-Mail **service@helmsauer-gruppe.de**
oder per Fax **0911- 9292 432**