FAQ IT-Sicherheit

Leitfaden für Gebäudedienstleister

Ausgabe Mai 2021 |

Herausgeber:
Bundesinnungsverband des Gebäudereiniger-Handwerks
Dottendorfer Straße 86
53129 Bonn
www.die-gebaeudedienstleister.de
T: +49-228-917750
Mail: biv@die-gebaeudedienstleister.de

Die Gebäudedienstleister
Bundesinnungsverband

Einleitung

Angriffe auf Computer und betriebliche Netzwerke nehmen rasant zu und führen zu erheblichen direkten und indirekten Schäden bei den Betroffenen. Und es sind bei Weitem nicht nur Großkonzerne Ziele und Opfer solcher Attacken, sondern es gelangen zunehmend auch mittelständische Unternehmen in den Fokus. „Die Frage ist nicht, ob eine Cyberattacke kommt, sondern wann“, so die realistische Einschätzung von Bundesinnungsmeister Thomas Dietrich.

Um seine Mitgliedsunternehmen bei den elementaren Vorkehrungen zur Verbesserung der eigenen IT-Sicherheit zu unterstützen und im Falle eines tatsächlichen Angriffs das Richtige zu tun, hat der Bundesinnungsverband des Gebäudereiniger-Handwerks eine neue Arbeitsgruppe IT-Sicherheit_Cybercrime ins Leben gerufen.

Mitglieder des Ausschusses für Technik und Betriebswirtschaft sowie IT-Expertinnen und -Experten aus Mitgliedsunternehmen erarbeiten gemeinsam Lösungsvorschläge: Wo liegen technisch die größten Angriffsflächen in Unternehmen? Welche Warnzeichen können Beschäftigte beachten? Welche Hard- und Softwarelösungen bieten Schutz? Und welche Möglichkeiten gibt es, im Schadensfall, die Auswirkungen für das Unternehmen so gering wie möglich zu halten.

Denn durch eine Cyberattacke droht der vollständige Verlust betrieblicher Daten, wie es auch aktuelle Beispiele aus der Branche gezeigt haben. Und dies selbst bei Unternehmen, die bereits zahlreiche Sicherungsmaßnahmen installiert hatten. Der resultierende materielle wie immaterielle Schaden kann immens sein, so dass die vorbeugenden Maßnahmen in ihrer Bedeutung nicht unterschätzt werden dürfen. Allein die Vorstellung, keinerlei Rechnungsdaten mehr zu besitzen oder sämtliche Daten der Beschäftigten rekonstruieren zu müssen, mag einen kleinen Hinweis darauf geben, welche Folgen ein solcher Angriff haben kann. Sie sind in der Regel nur unter enormem Aufwand oder via Datenrückkauf gegen Zahlung von Lösegeldern wieder zu erlangen. Das Thema kann und darf in seiner Bedeutung deshalb keinesfalls unterschätzt werden und betrifft Groß- wie KMU-Unternehmen mittlerweile gleichermaßen.

Mit dem vorliegenden ersten Leitfaden „FAQ IT-Sicherheit“ werden zunächst die wichtigsten Stellschrauben zusammengetragen, mit denen ein Betrieb die Grundlage für einen größtmöglichen Schutz bilden kann. Der Leitfaden dient in erster Linie dazu, für das Thema zu sensibilisieren und die vielfältigen Bausteine eines Sicherheitskonzeptes aufzuzeigen und zu erläutern. Allerdings ist das Thema heute derart komplex, facettenreich und anspruchsvoll, dass die dringende Empfehlung lautet, für die konkrete Umsetzung und Betreuung des Netzwerks entsprechende Experten hinzuziehen bzw. ein IT-Systemhaus mit der umfassenden Absicherung zu beauftragen.

Inhalt

Computer & Drucker

Kennwörter

Frage: Warum sind Kennwörter so wichtig und wie sieht ein sicheres Kennwort aus?

Kennwörter sind wichtige und zugleich sehr wirksame Stellschrauben, wenn es um das Thema Sicherheit der Firmen IT-Infrastruktur geht. Ein sicheres Kennwort entscheidet oft, ähnlich wie bei einem Einbrecher und einer Haustüre, ob der Hacker die offensichtlichste Einstiegsmöglichkeit ohne großen Aufwand überwinden kann, oder es nach einigen Misserfolgen bei einem anderen Haus versucht. Ein sicheres Kennwort sollte aus mindestens acht Zeichen und einer Kombination von Buchstaben, Zahlen und Sonderzeichen bestehen. Mit Zunahme der Komplexität der Schutzstufe sollte auch der Kennwortschutz anspruchsvoller gestaltet werden; Empfehlungen gehen in die Richtung, mindestens 16 Zeichen zu verwenden und diese z.B. als „Pass-Sätze“ zu bilden. Auch sollten Kennwörter niemals aufgeschrieben und in der Nähe des Arbeitsplatzes aufbewahrt werden.

Nützliche Links:

Empfehlungen des BSI (Bundesamt für Sicherheit in der Informationstechnik):

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html

Faktenblatt „Sichere Passwörter“, BSI:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Checklisten/sichere_passwoerter_faktenblatt.pdf?__blob=publicationFile&v=1

Aktuelle Betriebssysteme und Patchstände

Frage: Warum ist es so wichtig, dass alle Computer im Firmennetzwerk über aktuelle Betriebssysteme sowie aktuelle Patchstände verfügen?

Jeder Computer, welcher nicht über die aktuellsten Patches und die aktuellste Version der Software verfügt, ist ein potentielles Risiko. Hersteller von Programmen und Betriebssystemen arbeiten ständig an Updates, welche neben neuen Funktionen auch Sicherheitslücken innerhalb der Systeme schließen. Durch neue Funktionen ergeben sich zwangsläufig auch wieder Sicherheitslücken; demnach ist das Patch-Management eine Endlosspirale, die Unternehmen vor die Aufgabe stellt, sich laufend mit dem Thema in Bezug auf ihre IT-Infrastruktur zu beschäftigen. Gerade Computer, welche selten verwendet werden, beispielsweise Schulungslaptops oder Computer zur Zeiterfassung werden häufig im Hinblick auf ihre Aktualität vernachlässigt.

Moderne und regelmäßig gewartete Drucker

Frage: Sind Drucker auch potentielles Risiko?

Ja! Drucker müssen, genau wie Computer, ständigen Updates unterzogen werden, damit sie kein einfaches Einfallstor für potentielle Angreifer bieten. Drucker sind im Normalfall permanent und direkt mit dem Netzwerk verbunden und sind daher ein oft unterschätztes Gefahrenpotential.

Netzwerk

WLAN

Frage: Kann man bedenkenlos ein Firmen-WLAN betreiben?

Grundsätzlich schon, es empfiehlt sich aber zwischen einem internen und einem WLAN für Gäste zu unterscheiden. Sie sollten Ihr primäres WLAN grundsätzlich verschlüsseln (z.B. durch WPA2) und auch nur Geräte in das WLAN aufnehmen, welche Sie kennen. Dazu eignet sich auch die Verwendung eines MAC-Filters. Somit können nur Geräte in dem Netzwerk kommunizieren, die Sie durch die Eingabe einer Art Seriennummer auf Ihrem Router dazu autorisiert haben. Zusätzlich können Sie das Risiko durch die Nutzung eines Gäste-WLAN, welches komplett von Ihrer sensiblen IT-Infrastruktur abgeschieden ist, senken. Zusätzlich sollte die SSID (der Name des WLAN) nicht direkt erkennen lassen, dass es sich um das WLAN Ihrer Firma handelt. Somit wissen potentielle Hacker im ersten Moment gar nicht, welches der empfangenen WLAN-Signale auf Ihre Firma zurückzuführen ist.

VPN

Frage: Ist eine VPN-Verbindung nicht automatisch sicher?

Nein! VPN Verbindungen bergen, gerade zu Zeiten, in denen vermehrt Arbeitnehmer im Homeoffice arbeiten, große Risiken, da Sie einen Zugriff auf Ihr Netzwerk von überall, wo eine Internetverbindung besteht, ermöglichen. Daher ist es unerlässlich, dass Sie verschlüsselte VPN-Verbindungen verwenden (z.B. über den Einsatz einer Firewall). Das ist das Mindestmaß an Sicherheit, welches Sie in jedem Fall erreichen sollten. Grundsätzlich wird von IT-Experten empfohlen, eine zwei-Faktor Authentifizierung für VPN-Verbindungen einzurichten. Das heißt, dass sich jemand, der sich von extern mit Ihrem Netzwerk verbinden möchte, ein zweites Authentifikationsmedium angeben muss. Dies kann zum Beispiel ein Zahlencode sein, welcher in einer von Ihnen vorgegebenen App auf dem Smartphone angezeigt wird. Somit wird das Risiko, dass eine ungewünschte VPN-Verbindung zu Ihrem Netzwerk aufgebaut wird, stark minimiert.

Firewall

Frage: Ich habe eine Firewall, jetzt bin ich doch abgesichert – oder?

Das Thema Firewall ist sehr komplex und es gehören viele Faktoren dazu. Wichtig ist grundsätzlich, dass Ihr Netzwerk durch eine physikalische Firewall vor der Außenwelt geschützt wird. Hier gibt es zahlreiche Hersteller und Ausführungen. Je mehr (Sicherheits-) Aufgaben die Firewall übernimmt, desto teurer wird das Gerät aufgrund der benötigten Leistungsfähigkeit. Beispielsweise können leistungsfähige Firewalls die Anhänge eingehender E-Mails nach Viren durchsuchen und diese direkt aussortieren, bevor sie das Postfach Ihres Mitarbeiters erreichen (Fachbegriff: Sandbox). Auch können Firewalls den Besuch von Internetseiten überwachen und sofort ungewollte Downloads, Weiterleitungen auf schadhafte oder pornographische Internetseiten verhindern.

Der Einsatz einer Firewall wird allgemein als Standard angesehen.

VLAN

Frage: Was ist ein VLAN und warum wird es verwendet?

Ein VLAN ist die virtualisierte Form eines Netzwerks. Man unterteilt das physikalische Netzwerk virtuell in verschiedene Bereiche, im entferntesten Sinne vergleichbar mit einem Wassergraben um ein Schloss herum. Ein erfolgreicher Angreifer landet, nachdem er die erste Mauer überwunden hat, nicht direkt im Innenhof Ihres Unternehmens, sondern lediglich in einem Teilbereich, welcher nicht alle kritischen Daten und Informationen enthält.

Benutzerrechte (Active Directory)

Frage: Wir haben doch sichere Kennwörter, warum sind Benutzerrechte dann so wichtig?

Die Frage, welcher Benutzer auf welche Dateien Zugriff haben muss, sollten sich Unternehmer regelmäßig stellen. Grundsätzlich sollte man bei der Vergabe von Benutzerrechten eher die Tendenz beibehalten, so wenig Spielraum wie nur möglich zu vergeben. Ein Benutzer kann immer, auch mit einem sicheren Kennwort, gehackt werden und Daten abfließen lassen. In diesem Fall ist es wichtig, dass der Schaden durch vernünftig und logisch durchdachte Benutzerrechte gemindert wird. Auch im Hinblick auf eine unangenehme Trennung zwischen Arbeitnehmer und Arbeitgeber – Benutzerrechte spielen eine große Rolle im Hinblick auf die Sicherheit Ihrer Daten. Alte Benutzer, welche nicht mehr im Unternehmen genutzt werden, sollten zumindest deaktiviert, wenn schon nicht ganz gelöscht werden.

Serverlandschaft

Redundante Systeme

Frage: Ist mein Server nicht automatisch redundant, wenn ich eine Datensicherung verwende?

Die Frage nach der Redundanz ist auch immer eine Frage des finanziellen Invests. Eine Serverlandschaft läuft nicht redundant (also ausfallsicher), nur weil eine regelmäßige Sicherung der Daten erstellt wird. Wenn die Festplatte Ihres Servers einen plötzlichen Defekt bekommt, ersetzt und wiederhergestellt werden muss, vergehen angesichts der Masse an Daten unter Umständen mehrere Tage. Eine solche „down-time“ kostet viel Geld, da einige Mitarbeiter für diese Zeit unproduktiv sind oder im schlimmsten Fall einige Tage umsonst gearbeitet haben, da alle eingegebenen Daten zwischen der letzten Datensicherung und dem Ausfall der Festplatte verschwunden sind. Die Betreibung eines redundanten Systems – also zweier Server, welche sich gegenseitig in ihren Aufgaben ersetzen können – ist natürlich mit doppelten Hardwarekosten verbunden. Jeder Unternehmer, welcher von einem solchen Ausfall mit nur einem Server betroffen gewesen ist, wird jedoch bestätigen können, dass sich eine solche Investition in gewissen Szenarien rechnet.

Sichere Serverschränke

Frage: Ich habe doch einen Serverraum, reicht das nicht aus?

Nein, ein eigener – im besten Fall klimatisierter – Raum für die Server ist eine gute Grundlage aber erfüllt noch nicht alle Anforderungen zu dem wichtigen Thema der Zugangskontrolle. Server sollten grundsätzlich nicht im Büro eines Mitarbeiters oder lose in einer Abstellkammer stehen. Es ist wichtig, dass geeignete Serverschränke verwendet werden. Diese bieten neben dem Schutz vor Vandalismus gleichzeitig (und je nach Ausführung) Schutz vor Wasser, Feuer und für die Hardware

schädliche Temperaturen. Die Schränke sollten zu verriegeln sein und nur ausgewählte Personen sollten Zugang zu dem Herzstück Ihrer IT haben.

USV

Frage: Was ist eine USV und warum braucht man sie?

Eine USV (unterbrechungsfreie Stromversorgung) ist unerlässlich für Ihr Unternehmen. Im Prinzip handelt es sich hierbei um eine kleine Notstromeinheit, welche Ihre Serverlandschaft für kurze Zeit mit Strom versorgt, wenn in Ihrem Firmengebäude ein Stromausfall eintritt. Ein abruptes Abbrechen der Stromzufuhr kann die gesamte Serverlandschaft innerhalb weniger Sekunden vernichten. Tritt der schlimmste Fall ein, so wird kurzzeitig die Stromversorgung von der USV übernommen und es werden alle Geräte Ihrer Serverlandschaft behutsam heruntergefahren, ohne dass Daten verloren gehen oder die Hardware zu Schaden kommt. Auch kann eine USV Überspannungen der Leitungen, welche beispielsweise durch den Einschlag eines Blitzes in Ihrem Firmengebäude verursacht werden könnten, vor der empfindlichen und auf Gleichstrom angewiesenen Hardware bewahren. Es gibt sogar Modelle, welche Sie per SMS benachrichtigen, wenn etwas mit der Stromversorgung nicht stimmt – egal wann.

Virtualisierung

Frage: Was spricht für eine Virtualisierung von Servern?

Virtualisierte Server (also die Unterteilung eines physikalischen Servers in mehrere virtuelle Server) bieten diverse Vorteile und gehören mittlerweile zum Standard in der IT. Virtuelle Server sind einfacher zu warten, zu patchen und sorgen für viel Flexibilität. Ein Server wird langsam? Früher hätten Sie unter Umständen einen neuen Server kaufen müssen – einem virtualisierten Server teilen Sie einfach mehr Hardware-Ressourcen zu und innerhalb von fünf Minuten ist die Geschwindigkeit wieder so, wie sie gebraucht wird.

Software

Endpoint Protection

Frage: Hat nicht jeder Computer von Haus aus eine Anti-Viren-Software oder reichen nicht kostenfreie Versionen?

Anti-Viren-Software gibt es wie Sand am Meer. Grundsätzlich liefert Microsoft von Haus aus auch einen eigenen Virenschutz auf aktuellen Betriebssystemen (Windows 10). Die Entscheidung, auf welchen Hersteller gesetzt wird, obliegt immer den persönlichen Erfahrungen. Die meisten IT-Experten raten dazu, sich nicht auf kostenfreie Varianten zu verlassen und auf allen Computern im Netzwerk eine gekaufte Anti-Viren-Software zu installieren. Ähnlich wie bei dem Thema der Firewall gibt es auch in diesem Bereich verschiedene Ausführungen zu unterschiedlichen Preisen. Beispielsweise kann man gekaufte Software häufig mit verschiedenen sicherheitsrelevanten Einschränkungen (Policies) auf die Infrastruktur und Prozesses Ihres Unternehmens optimieren, um das maximale Maß an Sicherheit aus dem Viren-Scanner herauszuholen. Auch gibt es zahlreiche Add-ons wie die Verschlüsselung von Festplatten, wenn doch mal ein Außendienst-Notebook im Zug vergessen wird oder ein Firmenhandy aus der Umkleidekabine im Fitnessstudio gestohlen wird.

Weitere Add-ons sind beispielsweise Module, wie Schnittstellenkontrollen, die z.B. die unberechtigte Nutzung von USB-Sicks verhindern kann, oder auch Applikationskontrollen, die z.B. die unberechtigte Ausführung von Programmen und Scripts verhindern können.

Das sind alles Features, die eine kostenfreie Variante in der Regel nicht abdeckt.

Lassen Sie sich unbedingt dazu von Ihrem IT-Betreuer beraten, wenn Sie hier noch Handlungsbedarf bei sich erkennen.

MDM (Mobile-Device-Management)

Frage: Können Handys und Tablets auch von Viren befallen werden?

Es gibt schon einen Unterscheid zwischen Viren, die auf Computern ihr Unwesen treiben, und Viren, die es auf Mobilgeräte abgesehen haben. Bei letzterem ist das Ausmaß des verursachten Schadens zwar meist geringer, dennoch sollte der Part der Mobilgeräte nicht vernachlässigt werden. Firmeneigene Mobilgeräte sollten mit Hilfe eines Mobile-Device-Managements kontrolliert und geschützt werden. Beispielsweise können so verlorene Geräte über das Internet restlos gelöscht oder auch geolokalisiert werden. Auch werden mögliche Viren schneller erkannt und von dem Gerät entfernt.

Häufig wird das MDM mit der Endpoint Protection kombiniert. Gerne können Sie sich dazu auch beraten lassen.

End-of-Life

Frage: Was bedeutet End-of-Life und warum sollte man darauf achten?

Die Notwendigkeit der Aktualität der eingesetzten Software und der Betriebssysteme wurde bereits verdeutlicht. Große Hersteller kündigen häufig das so genannte „End-of-Life“ einer Software, also das Ende der Update-Versorgung seitens des Herstellers für ihre in die Jahre gekommenen Produkte an. Es ist wichtig, die Medien in dem Hinblick im Auge zu behalten oder sich zu dem Thema eng mit dem IT-Dienstleister zu verdrahten, damit die Notwendigkeit neuer Software oder Betriebssysteme nicht plötzlich und ungeplant auf Sie zukommt. Hier geht es auch um besser planbare finanzielle Belastungen, da der Neukauf eines Serverbetriebssystems schnell vierstellige Beträge kosten kann.

Software-Support

Frage: Sind Wartungsverträge wirklich notwendig?

Kurze Antwort: Ja. Wartungsverträge versorgen Ihre Software mit neuen Updates und heben somit das Level der Sicherheit permanent an.

Mitarbeiter

Frage: Kann man sich durch ausreichende Schutzmaßnahmen die Sensibilisierung der Mitarbeiter sparen?

Grundsätzlich gilt: Schutz durch Firewall, Virenscanner, Benutzerrechte und Co. sind eine solide Basis; die fachgerechte Schulung von Mitarbeitern ist trotz aller Vorkehrungen dennoch unerlässlich. Schulen Sie Ihre Belegschaft **regelmäßig** zu Themen wie:

- Vergabe eines sicheren Kennworts
- Wie erkennt man gefährliche E-Mails
- Wie erkennt man gefährliche Links

- Wem darf ich welche Daten senden (nach extern) und wann sollte ich mir eine Genehmigung vom Vorgesetzten einholen
- Besondere Aufmerksamkeit bei eingehenden Bewerbungen per E-Mail, insbesondere hinsichtlich der Anhänge (z.B. PDF-Dokumente)
- Es ist nicht peinlich und auch nicht schlimm, bei Unsicherheiten einen IT-Fachmann zu fragen
- Wie verhalte ich mich mit Daten (Papier und digital) im HomeOffice
- Wie werden Daten korrekt und sicher vernichtet

Backup

Häufigkeit

Frage: Wie oft sollte man seine Daten sichern?

Daten sollten jede Nacht inkrementell (also nur die Daten, die zum Vortag verändert oder hinzugefügt wurden) gesichert werden. Wöchentlich sollte ein volles Backup über alle Datenstände erstellt werden.

Speicherort

Frage: Wo sollten die gespeicherten Daten aufbewahrt werden?

Die Aufbewahrung der Daten sollte auf verschiedene Säulen verteilt werden. Daten können direkt im Unternehmen vorgehalten werden, damit sie schnell im Zugriff sind, wenn mal eine Datei wiederhergestellt werden muss. Die wöchentlichen, kompletten Sicherungen sollten zusätzlich außerhalb der Firma aufbewahrt werden, um im Falle eines Feuers im Firmengebäude keine verbrannten Datensicherungen in den Händen zu halten. Es bietet sich auch an, regelmäßige Datensicherungen in einem sicheren Cloud-Speicher online auszulagern (z.B. bei Ihrem IT-Dienstleister).

Regelmäßige Tests

Frage: Müssen die Sicherungen auch getestet werden?

Ein ganz klares: Ja! Auch in Datensicherungen können sich Fehler einschleichen und es wäre nichts ärgerlicher, als wenn die Datensicherung im Ernstfall unbrauchbar wäre, weil sie nie jemand ausgetestet hat. Daher ist es ratsam, die vorgehaltenen Sicherungen regelmäßig auszutesten. Es reicht in der Regel aus, diesen Test einmal pro Jahr durchzuführen.

Glossar

Active Directory	Die Benutzerverwaltung eines Netzwerks (Verwaltung von Benutzernamen, Kennwörtern, Berechtigungen)
Endpoint Protection	Fachbegriff für den Virenscanner, der auf den jeweiligen Computern installiert ist. Der Endpoint = "letzter Punkt" (der Computer), Protection = Schutz
MAC-Filter	Jedes internetfähige Endgerät besitzt eine eindeutige MAC-Adresse (bestehend aus Zahlen und Buchstaben). Ein MAC-Adressen-Filter sorgt dafür, dass sich nur auf dem Router eingetragene Geräte mit dem Internet verbinden dürfen. Alle anderen, nicht eingetragenen Geräte werden automatisch im Netzwerk blockiert
Patch	Verbesserungen von bestehender Software, z.B. zur Schließung von Sicherheitslücken
Ransomware	Bezeichnet eine bestimmte Kategorie von Computerviren (häufig gehören Verschlüsselungs-Viren zu dem Bereich Ransomware)
Sandbox	Simulation einer realen Serverumgebung, in welche die Funktion von (Mail-)Anhängen getestet werden.
VLAN	Abkürzung für Virtual local area network, ein virtuelles Netzwerk eines Unternehmens
VPN	Abkürzung für Virtual private Network, eine Verbindung zum (Firmen-)Netzwerk über das Internet
WPA2	Verschlüsselungstechnik für WLAN-Netze

Herausgeber:

Bundesinnungsverband des Gebäudereiniger-Handwerks
Dottendorfer Straße 86
53129 Bonn
www.die-gebaeudedienstleister.de
T: +49-228-917750
Mail: biv@die-gebaeudedienstleister.de