Einblicke in die IT-Sicherheit der Hörakustikbranche

Wenn nichts mehr geht

Mit der Betreuung von mehr als 200 Hörakustikfilialen im DACH-Raum hat der IT-Dienstleister ComputerSysteme Lonz in den vergangenen sieben Jahren tiefe Einblicke bekommen, an welchen Stellen es IT-technisch bei vielen Fachgeschäften hapert. Anhand konkreter Fallbeispiele, die einigen sicherlich bekannt vorkommen werden, gibt Geschäftsführer Emanuel Lonz Tipps und Tricks, wie sich die IT-Sicherheit in der Filiale verbessern lässt.

Und dann ist er plötzlich da – der große Blackout. Keine Software läuft mehr und alles bleibt bedrohlich still. Im Februar machten gehackte Server wieder weltweit Schlagzeilen. In Karlsruhe traf es acht Schulen, die der Sicherheitslücke mit dem Namen CVE-2021-21974 zum Opfer fielen. Weitere 77 Server mussten vom Netz genommen werden, weil das Ausmaß der Katastrophe nicht absehbar war. Die genannte Sicherheitslücke wurde auch einem neuen Kunden aus der Hörakustikbranche zum Verhängnis, der einen VMware-Server im Einsatz hatte. Durch den Hack verlor das Unternehmen alle Daten aus 18 Jahren Firmengeschichte.

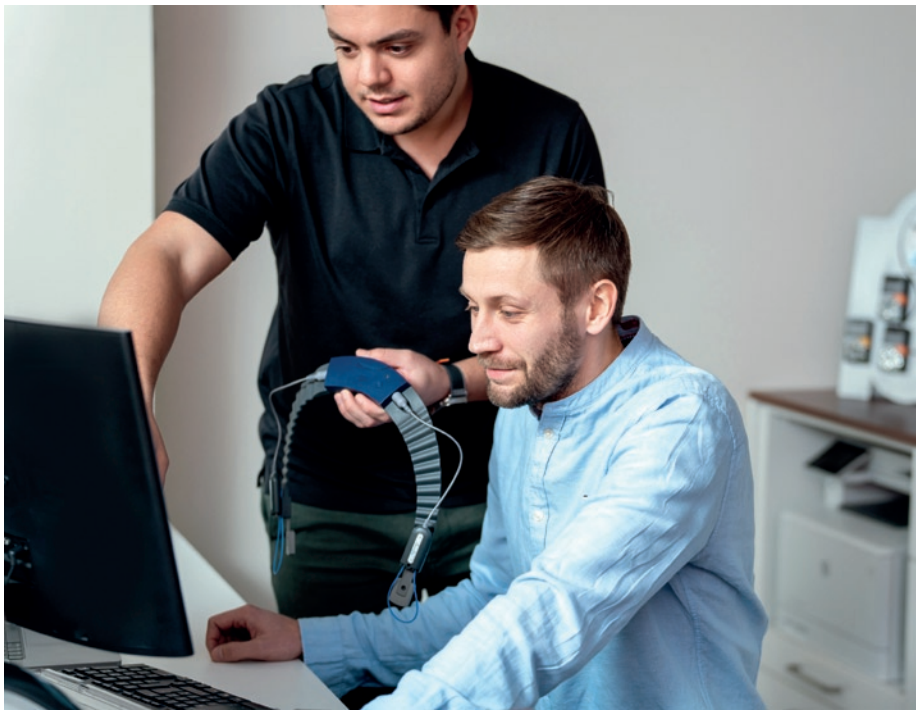
„Hallo, wer ist denn da am Telefon?“

Eine weit verbreitete Masche, um an relevante Daten zu kommen, ist das Social Engineering. Diese Form des Angriffs bezieht sich auf eine Methode der Täuschung und Manipulation, die von Angreifern verwendet wird, um sich Zugang zu vertraulichen Informationen oder Systemen zu verschaffen. Die Taktik besteht darin, den menschlichen Faktor in der Sicherheitskette auszunutzen. Die Opfer werden getäuscht, um sensible Informationen preiszugeben oder ungewollte Handlungen auszuführen (Phishing). Konkret haben wir das bei all unseren betreuten Branchen erlebt, vermehrt allerdings in der Hörakustikbranche. Diese zwei Beispiele aus unserer Praxis beschreiben das Phänomen Phishing besonders gut.

Phishing

Der erste Fall liegt schon ein paar Jahre zurück. Das Telefon klingelt bei einem Hörakustiker und es meldet sich ein vermeintlicher Mitarbeiter einer Branchensoftware. Der Hersteller habe mehrere E-Mails geschrieben, dass ein dringendes Programmupdate durchgeführt werden muss. Da nicht reagiert worden sei, müsse jetzt, am Freitag um 17:30 Uhr, das Update durch den Hersteller selbst durchgeführt werden. Ein Arbeiten am nächsten Tag sei sonst nicht mehr möglich, weil die Software dann nicht mehr funktioniere. Das wiederum habe einen Ausfall von mindestens drei Wochen zur Folge. Der Hörakustiker gibt die Zugangsdaten zur Wartungssoftware des Herstellers durch und bis 18:30 Uhr werden dem Hörakustiker die komplette Kundendatenbank entwendet und sein Server verschlüsselt. Die Lösegeldforderung betrug in diesem Fall 50 Bitcoin, was damals einem Wert von unter 300 Euro entsprach, aber dennoch eine stattliche Summe ist.

Im zweiten Fall rief eine ältere Dame bei einem Hörakustiker an und fragte nach dem Preis und den Einstellungen vom Hörgerät ihres Mannes. Die Mitarbeiterin gab der Anruferin bereitwillig Auskunft, da sie davon ausging, mit der Ehefrau zu sprechen. Drei Wochen später kam eine Abmahnung eines Anwalts und der Hinweis auf Anzeige bei der Datenschutzbehörde, weil einer fremden Person unbe-



IT-Support ist eine wichtige Maßnahme, um sich vor Cyberangriffen zu schützen. Foto: ComputerSysteme Lonz

rechtigterweise Auskunft über den Gesundheitsstatus des Mandanten erteilt worden sei.

Zugegeben, ein dramatischer, aber in der Praxis durchaus relevanter Fall. Welche Reaktion wäre in dieser Situation richtig gewesen? Ganz einfach, keine Auskunft zu geben. Man kann letzten Endes nicht mit Sicherheit sagen, ob die Person am anderen Ende der Leitung auskunftsberechtigt ist. Daher raten wir mit unseren externen Datenschutzbeauftragten allen Kunden, eine strikte Telefonrichtlinie einzuführen, damit so etwas nicht passieren kann.

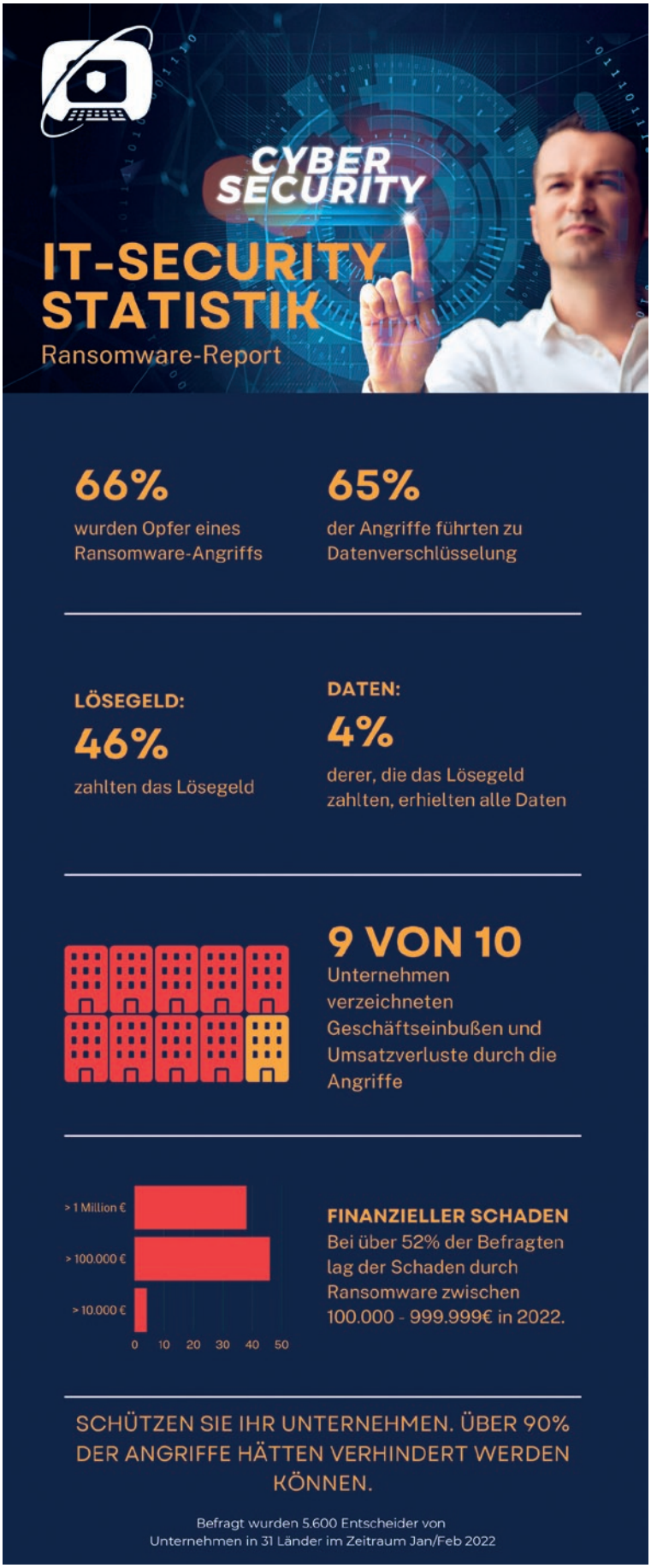
Die beste Lösung für das Problem ist, die Mitarbeiter jährlich durch Fachpersonal im Bereich IT und Datenschutz schulen zu lassen. So gibt man Mitarbeitern zumindest die Chance, sich in so einer Situation richtig zu verhalten. Gute IT-Dienstleister bieten jährlich Schulungen für Kunden an, um das Wissen aufzufrischen und über die häufigsten Angriffsmuster und Datenschutzfauxpas zu informieren. Ohne Schulung fallen in unseren Tests jährlich über 90 % der Neukunden durch. Erst nach den Schulungen herrscht eine Grundsensibilisierung, die zu korrekten Entscheidungen führen kann und die Durchfallquote sinkt auf unter 3 %.

Passwort, dich merk ich mir!

Ein Akustiker braucht im Durchschnitt täglich Zugriff auf 23 Portale und Websites, um seiner Arbeit entsprechend nachgehen zu können. In der Praxis bedeutet das: 23-mal das gleiche Passwort eingeben, um sich einzuloggen. Wer soll sich das sonst alles merken? Die genutzten Passwörter wie Hans67, Lübeck99 oder der Kombination aus Firmennamen und Postleitzahl finden hierbei Verwendung, um wichtige Zugänge zu E-Mails, Branchensoftware und Kundenportal zu schützen. Ist das sicher? Wie zu erwarten, ist es das nicht. Die Grundregel lautet daher: Wenn man sich ein Passwort merken kann, dann ist es nicht sicher genug.

Häufig ändert man seine bisherigen Passwörter in sichere wie beispielsweise 2G7@4wvBy. Keine Frage, dass so ein Passwort sicher ist. Doch wodurch wird auch dieses Passwort zu einem unsicheren Passwort? Wie bereits zu erahnen: die Verwendung des Passworts in mehreren Portalen.

Passwörter wurden so konzipiert, dass sie einmalig verwendet werden. Das Problem wiederholter Verwendung liegt auf der Hand. Wird nämlich nur eines der 23 Portale und Websites aus dem eigenen Browser gehackt und das Passwort mit der E-Mail-Adresse entwendet, kann man davon ausgehen, dass intelligente Hacker



Zahlen und Fakten zur IT-Sicherheit

Abbildung: Sophos Ransomware Report 2022

diese Kombination auf Millionen von Portalen weltweit ausprobieren. Die Server dokumentieren dann, wo eine Anmeldung erfolgreich war und dann werden Bankdaten, Kundendaten und Mitarbeiterinformationen abgezogen, ohne dass jemand dies bemerken würde.

Die beste Lösung für dieses Problem ist, einen Passwortmanager wie Lastpass oder Bitwarden als Plugin für den Browser zu verwenden. Diese Software verwaltet nicht nur Passwörter sicher verschlüsselt in der Cloud, sie prüft zusätzlich auch, ob die verwendeten Passwörter an irgendeiner Stelle aufgetaucht und daher nicht mehr sicher sind. Zudem haben diese Systeme einen eigenen Passwortgenerator eingebaut, sodass bei der Anmeldung auf einer Website mit nur einem Klick ein einmaliges und sicheres Passwort erstellt und direkt gespeichert wird. Wenn man dann noch bei einem Dienstleister einen Wartungsvertrag hat, der die Sicherheit überwacht, dann lässt sich das soeben erzeugte Kennwort nicht einmal kopieren. Das führt dazu, dass das Passwort außer dem System niemand kennt und bei einem Mitarbeiterwechsel nicht alle Passwörter geändert werden müssen. Das ist Passwortsicherheit auf höchstem Niveau ohne große Investition.

IT auf Wolke 7

Die Trendrichtung der IT ist klar: Es geht in die Cloud. Die Cloud hat enorme Vorteile gegenüber lokal gehosteten Servern innerhalb der Filiale. Die Cloud ist schnell bereitgestellt, bei Bedarf gut erweiterbar, für mobiles Arbeiten geeignet und sehr flexibel. Doch wie steht es eigentlich um die besonders wichtigen Themen wie Sicherheit, Datenschutz und Verfügbarkeit?

Sicherheit ist wohl das entscheidendste Thema für oder gegen die Cloud. Bis vor zwei Jahren haben wir den von uns betreuten Hörakustikern von der Cloudnutzung eines bestimmten Herstellers einer Branchenlösung abgeraten, weil wir diese als nicht sicher erachtet haben. Wir haben den Hersteller mehrfach auf unsere Bedenken aufmerksam gemacht und schlussendlich hat ein Wechsel der IT-Leitungsebene dazu geführt, dass wir nun auch diese Cloud-Lösung empfehlen können.

Voraussetzungen für mehr Sicherheit

Abbildung: wwwczlonz.de

Die Frage des Datenschutzes ist in diesem Zusammenhang ebenso wichtig, denn als Hörakustiker haftet man, wenn Daten abhandenkommen. Die Verarbeitung von personenbezogenen Daten in der Cloud kann bedeuten, dass die Kontrolle über die Daten an einen Drittanbieter übergeben wird, was wiederum Datenschutzfragen aufwirft. Es ist wichtig sicherzustellen, dass die Cloud-Provider die Anforderungen an den Datenschutz erfüllen und dass die Nutzungsbedingungen vertraglich vereinbart sind. Außerdem ist der Serverstandort der genutzten Cloud zu beachten. Daten und auch gerade Backups der Systeme sollten die EU keinesfalls verlassen. Dies sollte anhand der Auftragsdatenverarbeitungsverträge nachgeprüft werden. Im Zweifel einfach den Datenschutzbeauftragten der Software anrufen. Bei der Nutzung von Office stehen die verwendeten Microsoft-Server sehr wahrscheinlich in den USA, wenn nicht explizit der Serverstandort Deutschland vereinbart wurde. Auch dies wäre eine unzulässige Datenverarbeitung.

Das letzte Problem ist die Verfügbarkeit der Daten. Hier gibt es zwei Seiten: die eigene und die der Cloud. Bei der Cloud ist der Fall klar: Der Betreiber muss für ein hohes Maß an Ausfallsicherheit sorgen. Informationen über diese Konzepte werden zumeist auch mit dem Auftragsdatenverarbeitungsvertrag geliefert, der mit jedem abgeschlossen werden sollte, der die Unternehmensdaten in irgendeiner Art verarbeitet und nicht zum Unternehmen gehört.

Das weitaus größere Problem in der Praxis ist die Verfügbarkeit in der Filiale selbst. Die IT-Sicherheit, die Stabilität der Internetverbindung sowie die Wartung der eingesetzten Rechner spielen hier eine zentrale Rolle, was von den meisten unterschätzt wird. Auch aus der Cloud können Daten lokal von Angreifern gestohlen werden, das ist mittlerweile schon oft mit Erfolg praktiziert worden. Es gilt also achtsam zu sein und alle Technik zeitnah zu warten.

Updates, Treiberpatches und Antivirensoftware

Der in der Einleitung beschriebene Fall des Hörakustikers, dessen Server im Februar 2023 verschlüsselt wurde, stellt einen Meilenstein zum Thema Ransomware dar. Bis vor Kurzem waren Verschlüsselungstrojaner nur auf Systemen bekannt, die unter Windows arbeiten. Nun wissen wir, die Angreifer werden effektiver und nutzen Ziele, an die bislang keiner gedacht hat. Weltweit waren von dieser Sicherheitslücke der VMware-Server rund 84 000 Server betroffen, davon etwa 7 000 allein in Deutschland [2]. VMware ermöglicht es, einfach ausgedrückt, auf nur einem Server mehrere kleine Server getrennt voneinander zu betreiben.

Im beschriebenen Fall wurde, wie fast immer bei solchen Angriffen, zu Beginn des Wochenendes mit dem Verschlüsseln der virtuellen Festplatten begonnen. Die drei laufenden Windows-Server auf dem VMware-Host wurden komplett verschlüsselt. Der Montag war dann für den Hörakustiker ein Schock, denn nichts ging mehr. Alle Systeme meldeten, dass eine Anmeldung nicht mehr möglich sei, Server nicht erreichbar seien und keine neuen E-Mails geladen werden könnten. Der Blick auf den Server klärte das Desaster dann auf: Lösegeld wurde erpresst, wenn man an seine Daten wollte. In seiner Panik rief der Hörakustiker einen IT-Dienstleister im Ort an, der den Server abholte. Dieser formatierte beim Versuch, das RAID (Festplattenkopie) des Servers wiederherzustellen, aus Versehen die Festplatten und die Daten waren weg. Das letzte Update war, wie auch das letzte Update des Servers, im Jahr 2020 gelaufen. Über einen befreundeten Hörakustiker kam er zu uns, aber auch wir konnten nach dieser Verkettung unglücklichster Umstände keine Hilfe mehr leisten, da auf den Festplatten keinerlei Daten mehr vorhanden waren.

Inzwischen arbeitet dieser Hörakustiker seit einem Monat in der Cloud und fängt wieder ganz von vorne an, da er keinerlei Kundendaten mehr hat. Der finanzielle Schaden ist immens und das Verfahren bei der Datenschutzbehörde läuft. Dieser Fall schildert eindrücklich, zu welchem enormen Schaden nicht gewartete und unbetreute Systeme für alle Beteiligten führen können.

Die beste Lösung für diese Problematik besteht darin, alle verfügbaren Updates der Treiber und Software auf den eigenen Systemen zu installieren. Zunächst sollte man einen Computer testen und anschließend alle weiteren PCs patchen. Vorsicht ist bei Kabinen-PCs geboten. Hier sollten zuvor Back-ups erstellt werden, da es in der Praxis nicht selten vorkommt, dass Updates beispielsweise Noah-Datenbanken beschädigen. Windows-Updates sollten installiert werden, sobald sie verfügbar sind. Wichtig ist, eine professionelle Antivirensoftware zu nutzen. Freeware und sehr preiswerte Programme unter 50 Euro im Jahr werden keinen ausreichenden Schutz gegen alle Bedrohungsarten liefern können, da der bezahlte Preis nicht annähernd die Kosten der notwendigen Leistung deckt. Bei täglich 40 000 neuen Malware Samples allein bei Sophos Labs kann man sich vorstellen, wie wichtig es ist, auf aktuelle Daten zuzugreifen. Eine Malware, die erst nach acht Wochen kostenfrei zur Erkennung freigegeben wird, wird im Zweifel nicht mehr vor einem Angriff schützen können.

Der IT-Dienstleister sollte, wenn er auf Hörakustiker spezialisiert ist, selbst ein Testsystem haben, auf dem er Updates vor der Installation prüfen kann. So kann man sicher sein, dass die Systeme nach den Updates weiterhin wie gewohnt funktionieren und keine Daten verloren gehen.

Fazit

Dieser Beitrag vermittelt einen kleinen Einblick in die häufigsten Schwachstellen von IT-Systemen der Hörakustikbranche. Vor dem Hintergrund des Datenschutzes und der Verarbeitung von Gesundheitsdaten durch Hörakustiker ist das aufgezeigte Schutzniveau keinesfalls als nice to have anzusehen. Hörakustiker sind hier in der Pflicht, ihre Systeme so abzusichern, dass nach aktuellem Stand der Technik kein fremder Dritter eindringen kann (Art. 32 Datenschutz-Grundverordnung (DSGVO)).

Es wird deutlich, dass dies nur ein kleiner Ausschnitt der Bandbreite von potenziellen Angriffen ist, von dem auch die eigene Filiale betroffen sein kann. Das Sicherheitsniveau lässt sich stark verbessern, wenn die genannten Punkte beherzigt werden. Wichtig ist, dass Mitarbeiter die Chance erhalten sollten, sich bei Schulungen zum Thema IT-Sicherheit und Datenschutz so fortzubilden, dass sie nicht länger das schwächste Glied in der Kette sind. Komplexe Passwörter sollten genutzt werden und jeweils nur einmalig für einen Dienst verwendet werden. Um die daraus resultierenden Schwierigkeiten zu meistern, hilft ein Passwortmanager, der sich direkt in den Browser integrieren lässt. Eine Entscheidung für Cloud-Lösungen ist dann sinnvoll, wenn man nach eingehender Prüfung des Anbieters zum Entschluss kommt, dass die angebotene Lösung den Datenschutz- und Sicherheitsrichtlinien entspricht. Mithilfe von System- und Windows-Updates sowie qualifizierter Sicherheitssoftware lassen sich die Systeme in der Filiale sichern. Der IT-Dienstleister sollte die Systeme entsprechend überwachen, am besten in einem 24/7-Service, um Veränderungen in den Netzen vor allem an Wochenenden und nachts sofort zu bemerken und eingreifen zu können. Dienstleister und Softwarehersteller sollten IT-Sicherheitskonzepte zeigen und erklären und Auftragsdatenverarbeitungsverträge sollten beim Verlassen der Filiale abgeschlossen sein.

IT-Sicherheit und 24/7-Wartung einer Filiale kosten weniger als die Marge eines einzigen Kassenhörgeräts. Der eigene Ruf und die Daten sind die Grundlage für den wirtschaftlichen Erfolg. Daher sollte nicht an der falschen Stelle gespart werden. Statt dessen ist es sinnvoll, die Möglichkeit zu nutzen, sicheres Arbeiten in der Filiale als Standard einzuführen.

Literatur

[1] Security Insider (2023) https://www.security-insider.de/cyberattacke-auf-vmware-esxi-server-trifft-auch-deutschland-a-b86d98f290a68b044f-34671820c8b96e/ (Stand: 24.02.2023)

[2] Channelpartner (2023) https://www.channelpartner.de/a/was-sich-aus-dem-angriff-auf-vmware-esxi-lernen-laesst,3616169 (Stand: 24.03.2023)

Emanuel Lonz, Geschäftsführer,
ComputerSysteme Lonz