Immer mehr Hacking-Angriffe

WIE STEHT ES UM DIE DATENSICHERHEIT IN DER HÖRAKUSTIK-BRANCHE?

Getty Images

Gehackt wird alles, was greifbar ist - egal, ob es sich um Daten eines Ein-Mann-Betriebs oder eines Unternehmens mit 20.000 Mitarbeitenden handelt.

Im Februar 2023 legte eine internationale Cyber-Angriffswelle mehrere Hundert deutsche Einrichtungen lahm. Die Sicherheitslücke einer Software, welche die Hacker ausnutzten, war eigentlich seit zwei Jahren bekannt. Doch viele Unternehmen gehen einfach zu fahrlässig mit Cybersicherheit um, meint IT-Dienstleister und Experte Emanuel Lonz.

Katrin Schneider

Audio Infos (AI): Herr Lonz, Ihre Firma mit Hauptsitz im südpfälzischen Gleiszellen-Gleishorbach betreut mittlerweile Hörakustiker*innen in ganz Deutschland, Österreich und der Schweiz. Wie ist die Branche Ihrer Erfahrung nach aufgestellt, was Datensicherheit angeht?

Emanuel Lonz (EL): Unserer Erfahrung nach sind Akustiker eher schlecht aufgestellt, wenn es um IT-Sicherheit geht. Unsere interne Statistik zeigt, dass 2022 über 70 Prozent aller Neukunden aus dem Bereich Akustik bereits Schadsoftware auf ihren Computern installiert hatten,

ohne dies zu bemerken. Und ganze 13 Prozent der Neukunden befanden sich im Moment der Vertragsanbahnung in einem Ransomware-Angriff. Besonders fallen uns zwei Problemgruppen bei den Akustikern auf: Die eine Gruppe setzt auf eigenes Hosting der Branchensoftware und hat dafür einen eigenen Server. In allen bisher gesehenen Fällen sind diese Server unzureichend gesichert, was auch im Sinne der DSGVO höchst problematisch ist. Die andere Gruppe ist bereits den Schritt in die Cloud gegangen und fühlt sich sicher. Es wird allerdings nicht bedacht, dass beispielsweise die komplette E-Mail-Kommunikation über die PCs weiterläuft. Ein Ausfall an dieser Stelle hat unweigerlich den Stillstand der Filiale zur Folge. Und auch diese PCs können genutzt werden, um die Daten aus der Cloud abzuziehen. Es ist also ein Teufelskreis, der unterbrochen werden muss. Dafür braucht es ausgereifte Sicherheitskonzepte.

AI: Was sind die häufigsten Datensicherheitsprobleme, auf die Sie in der Branche treffen?

EL: Eines der Probleme sind die eingesetzten Antiviren-Systeme: Entweder sie sind kostenlos und sorgen, mit Ausnahmen, selbst dafür, dass Daten abgezogen werden. Oder sie sind sehr günstig und decken nur einen Bruchteil der nötigen Sicherheitsaspekte ab. Die Hauptursache für erfolgreiche Hacking-Angriffe ist aber das Fehlen von fortlaufenden Wartungen der Systeme. Im besten Fall müssen in Echtzeit die Log-Dateien (Anm. d. Red: Protokolldateien) eines PCs ausgewertet werden, um Angriffe direkt zu erkennen. Wenn Kunden auf einen IT-Dienstleister zählen, der erst im Notfall zur Stelle ist, dann bedeutet das, dass die Systeme nahezu dauerhaft verwundbar sind. Doch ist der Angriff da, ist es meist zu spät. Daher werden feste Wartungsverträge seit Jahren zum Standard in der Akustikbranche.

Simon Rühl

IT-Sicherheitsspezialist Emanuel Lonz gründete 2006 seine Firma ComputerSysteme Lonz und betreut seit circa acht Jahren auch Hörakustiker*innen.

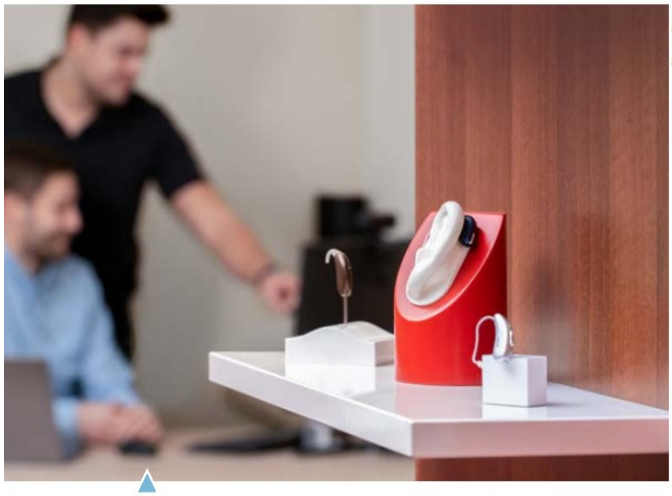
AI: Hacker-Angriffe auf den Bundestag oder große Firmen machen Schlagzeilen. Wie sehr ist der Mittelstand betroffen und wer hat Interesse an diesen Daten?

EL: In den letzten zehn Jahren haben wir einen Wandel der Angriffsziele gesehen, weg von genau geplanten Cyberangriffen auf Einrichtungen, Unternehmen und Behörden, hin zu weltweitem Ausschütten von Schadsoftware. Gehackt wird alles, was ein einfaches Ziel ist: ein Ein-Mann-Betrieb genauso wie ein Unternehmen mit 20.000 Mitarbeitern. Wenn der Hacker sich Zugang zum Netzwerk verschafft hat, dann schaut er sich automatisiert mit seiner Software heimlich und vorsichtig um. Er prüft, in welcher Branche er gelandet ist, welche Dateien täglich bearbeitet werden und schaut sich häufig durch Bildschirmfotos an, was auf den PCs den ganzen Tag passiert. Je interessanter ein Unternehmen ist, desto ruhiger verhält er sich, um möglichst viele Daten abzugreifen. Ist dieses Ziel erreicht, verschlüsselt er die Systeme und die Erpressungsphase beginnt. Es heißt dann „Bezahle, ansonsten bekommst du deine Daten nicht wieder" oder auch „ansonsten melden wir deine mangelnde IT-Sicherheit bei der Datenschutzbehörde, und du musst mit Strafe rechnen". Gleichzeitig werden die Daten nach unseren Erkenntnissen meist schon im Darknet angeboten. Da landen dann Kundendaten bei der Konkurrenz und der Gehackte wundert sich, weshalb die Bestandskunden immer weniger werden. Interessenten für Gesundheitsdaten gibt es viele. Das wird schnell existenzbedrohend.

Was ist zu tun bei einem Cyberangriff?

Der internationale Cybersecurity-Anbieter Sophos empfiehlt:

- Installation und Pflege hochwertiger Schutzmaßnahmen im gesamten Unternehmen sowie regelmäßige Sicherheitskontrollen.
- Aktive Suche nach Bedrohungen durch Spezialisten, um Angreifer zu identifizieren und zu stoppen.
- Härtung der IT-Umgebung, indem gefährliche Sicherheitslücken aufgespürt und geschlossen werden.
- Auf das Schlimmste vorbereitet sein: Unternehmen sollten bei einem Cybervorfall auf einen Notfallplan zurückgreifen können.
- Erstellen von Back-ups und Testen der Wiederherstellung.



Simon Rühl

Ein Hacking-Angriff kann den totalen Stillstand eines mittelständischen Betriebes zur Folge haben. Dann können oft nur noch Cybersecurity-Experten helfen.

AI: Was für Konsequenzen kann ein Angriff auf das System eines kleinen oder mittelständischen Unternehmens haben?

EL: Die Bandbreite an Konsequenzen ist nahezu unendlich. Wir hatten den Fall, dass wir ein infiltriertes System bekamen und wir den Einbrecher ausschließen konnten, bevor er die Systeme verschlüsselte. Wir haben aber auch Kunden, bei denen sogar wir als Spezialisten machtlos sind, weil die Trojaner schon alles verschlüsselt haben. In diesen Fällen prüfen wir die Festplatten und können manchmal auch nur noch hoffen, dass wir Daten aus guten Backups wiederherstellen können. Der schmerzliche Teil eines solchen Angriffs sind immer die Kosten: für Betriebsausfall, Wiederinbetriebnahme, Strafen durch die Datenschutzbehörde... Ein Akustiker mit einem Jahresumsatz von 500.000 Euro kann hier beispielsweise schnell mit einer Strafe von bis zu 20.000 Euro belegt werden, wenn er nicht nachweisen kann, dass seine Geräte und Netze entsprechend gängigen Standards gesichert waren. Das haben wir in der Praxis schon so erlebt. Auch führt ein Imageverlust von Unternehmen nicht selten zu Geschäftsaufgaben, weil die informierten Kunden keinerlei Verständnis dafür zeigen, dass ihre Gesundheitsdaten nun im Internet herumgeistern.

Es ist ein Teufelskreis, der unterbrochen werden muss. Dafür braucht es ausgereifte Sicherheitskonzepte.

AI: Sollte das Worst-Case-Szenario eintreten und man Opfer einer Cyberattacke sein: Was ist zu tun?

EL: Die allerwichtigste Regel ist: PCs und Server ausschalten. Was PCs brauchen, um die Verschlüsselungstrojaner auszuführen, ist Strom. Daher sofort den Stecker ziehen, auch am Router. Der zweite Schritt heißt: Kontakt aufnehmen mit Spezialisten. Wenn wir angerufen werden, bauen wir die Computer auseinander, lesen die Festplatten aus und erstellen Kopien im Labor. Damit retten wir zumindest den Stand der Daten bis zum Ausschalten der Computer. Anschließend werden Festplatten genau untersucht, wir überprüfen den ausgeführten Schadcode und können dadurch Rückschlüsse ziehen, was auf dem Computer passiert ist. Kennt man das Muster, kann man entschlüsseln. In manchen Fällen ist Ransomware allerdings so neu, dass diese Muster noch nicht bekannt sind, dann gibt es nur noch wenige Möglichkeiten, an die Daten zu gelangen. Im dritten Schritt ist es meist die sicherste und preiswerteste Variante, die PCs auszutauschen – am besten mit eigens entwickelten Systemen für die Branche. Diese werden dann aufgesetzt und mit den alten, gesäuberten Daten bespielt, das Netzwerk abgebaut und sicher neu aufgebaut. Im besten Fall dauert der Prozess vom Anruf bis zur Wiederaufnahme des Filialbetriebs fünf Tage. Dann folgt der letzte und wichtigste Schritt: Da statistisch gesehen 60 Prozent der Firmen, die angegriffen wurden, in den nächsten zwölf Monaten nochmals mit einem massiven Angriff rechnen müssen,

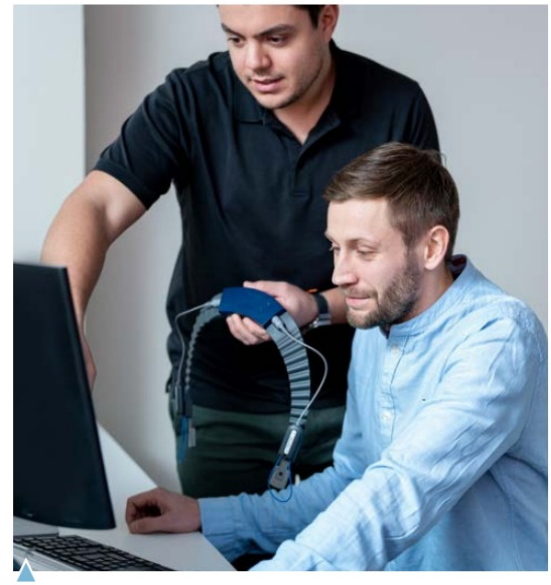
Cyberangriffe auf deutsche Unternehmen: Wie häufig, wie teuer?

Die jährliche internationale Sophos-Studie „State of Ransomware" ergab 2022 für das Vorjahr, dass 67 Prozent der in Deutschland befragten mittelständischen Unternehmen von Ransomware betroffen waren, im Jahr 2020 waren es noch 46 Prozent. Es zahlten 42 Prozent der deutschen Unternehmen, deren Daten verschlüsselt worden waren, das Lösegeld – im Durchschnitt 253.160 Euro, fast doppelt so viel wie 2020. Ein Ransomware-Angriff kann verheerende Konsequenzen haben. 92 Prozent der deutschen Unternehmen sahen ihre Betriebsfähigkeit beeinträchtigt, 84 Prozent der Opfer erlitten aufgrund des Angriffs Geschäfts- und/oder Umsatzeinbußen. Nach Statistiken des Forschungsunternehmens B2B International im Auftrag des Anbieters für Sicherheitssoftware Kaspersky Lab fallen für unmittelbare Schadensbegrenzung und präventive Maßnahmen nach einem Angriff im Schnitt für ein großes Unternehmen Kosten von 495.000 Euro an, für ein kleines oder mittelständisches Unternehmen 38.000 Euro.

Was passiert bei einem Hacking-Angriff?

Die grundlegenden Begrifflichkeiten sollten heute niemandem mehr fremd sein: Ein Hacking-Angriff ist der Versuch, von außen in Geräte wie Computer/Smartphones oder in ganze Netzwerke einzudringen. Dies kann zum Beispiel über Phishing-Mails (oder sogenanntes Smishing per SMS) geschehen, wenn das Opfer einen Link anklickt, aber auch über USB-Sticks, schwache WLAN-Verbindungen oder unsicher konfigurierte Netzwerke. Gezielt eingesetzte oder sich selbst verbreitende Malware (Schadsoftware) kann u.a. Server lahmlegen, Betriebssysteme schädigen und zu Datenverlust führen. Sie lässt sich in drei Klassen einteilen: Computerwürmer, Computerviren und Trojaner. Letztere tarnen sich häufig als nützliche Programme, die dann nachträglich andere Schadsoftware einschleusen. Ein Verschlüsselungstrojaner (Ransomware) kann Computerinhabern den Zugriff auf Daten verwehren. Für die Entschlüsselung wird dann Lösegeld erpresst – oft ohne dass eine Datenrückgabe gewiss ist. Die Empfehlung der Behörden lautet, kein Lösegeld zu zahlen.

sollten im Nachhinein starke Sicherheitsvorkehrungen getroffen werden, die dem standhalten. Erst dann merken viele Unternehmen, dass es sich lohnt, in IT-Sicherheit zu investieren – damit dieser Ransomware-Angriff der letzte gewesen ist in ihrer Firmengeschichte.



Simon Rühl

Emanuel Lonz gibt seinem Kundenstamm auch persönliche Tipps, wie das Sicherheitskonzept des eigenen Geschäftes verbessert werden kann.