MEINKAUFSTADT Wien
meinkaufstadt.wien
Eine Initiative der Wirtschaftskammer Wien

Cybercrime: Lassen Sie sich nicht in die Daten schauen!

Kriminalität im Internet nimmt zu. Die beste Versicherung gegen Angriffe von Hackern ist die Prävention.

12.04.2022, 15:38

© JUERGEN FAELCHLE/SHUTTERSTOCK

Von einer Nacht auf die andere waren alle Daten weg", schildert Peter Schrattenholzer, Geschäftsführer von Attensam Wien. Der Grund: Das Wiener Unternehmen mit Niederlassungen in ganz Österreich wurde gehackt. „Alle Server waren verschlüsselt. Wir hatten keinen Zugang mehr zu irgendwelchen Daten. Von Personaldaten, Telefonnummern, sämtlichen Kundendaten bis hin zu den Zutrittssystemen – alles war weg", erzählt Schrattenholzer vom Hackerangriff, der sich Ende 2020 abgespielt hat. Doch damit nicht genug: „Die Hacker haben auch eine Lösegeldforderung an uns gestellt – eine Summe im mittleren sechsstelligen Bereich", schildert er. Dank der Zusammenarbeit mit einer IT-Firma, die Schrattenholzer über Umwege gefunden hat, wurde diese Summe nicht den Cyberkriminellen überwiesen, sondern zur Gänze in die Sicherheit des Attensam-ITSystems gesteckt. „Der Schaden war natürlich trotzdem groß - wir haben mehrere Wochen gebraucht, um ein neues IT-System aufzubauen", erklärt Schrattenholzer. Unternehmen, die bisher noch verschont geblieben sind, rät er: „Prävention ist das Um und Auf. Es lohnt sich, Geld in die Hand zu nehmen, um einerseits laufend technisch aufzurüsten, und andererseits, um Mitarbeiter zu schulen - nur so kann man der Eintrittstür für Cyberkriminelle einen doppelten Balken vorschieben", betont er. „Im Falle eines Angriffs ist es immer gut, einen Profi zur Seite zu haben, der einen da durchführt und unterstützt. Und: Vielleicht sollte man sich überlegen, ob man manche Akten künftig auch wieder in Papierform ablegt."

„Daten sind kostbar: Ein Backup kann den Betrieb vor dem Untergang retten."

Cybercrime-Fälle steigen stark an

Die Firma Attensam ist eine von vielen betroffenen Betrieben, die Opfer von Cyberkriminellen wurden. Alleine im Vorjahr wurden österreichweit 46.179 Cybercrime-Fälle angezeigt - um ein Drittel mehr als im Jahr 2020 und um satte 50 Prozent mehr als noch im Jahr 2019. „In Wien stieg die Zahl 2021 um 22,4 Prozent auf insgesamt 17.068 Fälle", hebt Martin Heimhilcher, Wirtschaftskammer Wien-Obmann der Sparte Information und Consulting die steigende Bedrohung für Wiens Unternehmen vor. „Vor allem Klein- und Mittelunternehmen sind für die Täter angreifbarer, weil sie meist keine Ressourcen haben, um eigene IT-Security Abteilungen einzurichten." Den Grund für den rapiden Anstieg sieht Heimhilcher im Digitalisierungsschub, den die Coronakrise ausgelöst hat: „Die Coronakrise ist als Turbo für die Digitalisierung zu sehen. Das öffnet auch das Einfallstor für Cyberkriminelle weiter."

Hacker hinterlassen Spuren

Attensam ist einem Ransomware-Angriff zum Opfer gefallen. Dabei verschlüsseln Schadprogramme Daten. Danach erpressen Hacker Lösegeld für die Entschlüsselung. „Die meisten Cybercrime-Angriffe auf Betriebe sind Ransomware zuzuordnen", sagt Erhard Friessnik. Er leitet das Cybercrime Competence Center (C4) des Bundeskriminalamts. Dort ermitteln unter anderem Experten für elektronische Beweismittelsicherung und IT-Forensik. Friessnik rät Betrieben, Cyber-Angriffe immer zur Anzeige zu bringen, auch wenn man ein gutes Backup- System und gute IT-Betreuung hat: „Jeder Täter hinterlässt Spuren. Den perfekten Hack gibt es ebenso wenig wie den perfekten Mord. Je mehr Spuren wir finden und vergleichen können, desto eher können Täter ausgeforscht werden." Was die Ermittlungen schwierig mache sei, dass kaum Einzeltäter hinter den Angriffen stehen. „Wir haben es hier mit organisierter Kriminalität zu tun, die in mehrere Schritte eingeteilt wird: Einer schreibt eine Verschlüsselungs-Software - das ist an sich nicht strafbar -, ein anderer verschickt SMS. Erst das kompakte Konstrukt ergibt eine strafbare Handlung", so Friessnik. Betriebe, die erpresst werden, können von der Erfahrung und den internationalen Kontakten des C4 profitieren, wenn sie es sehr früh einbinden. „Ist der Fisch im Netz, dann tickt die Uhr. Je mehr Zeit verstreicht, desto mehr Druck bauen die Täter auf und desto teurer wird es. Wir helfen, eine Strategie zu entwickeln, beispielsweise, dass man verlangt, gewisse Daten freizuschalten, um einen Bluff auszuschließen", sagt Friessnik. Leider würde die Polizei meist als letzte Instanz kontaktiert, was ihre Arbeit erschwere. „Wir helfen, dass Betriebe zu ihrem Recht kommen. Doch die Daten wiederherstellen, das können wir nicht", so Friessnik. Neben der dringenden Empfehlung, Anzeige zu erstatten, ist ihm ganz wichtig, dass Betriebe sensibel im Umgang mit ihren Daten und in der Kommunikation mit Partnern sind, die sie noch nicht kennen.

TUN, WENN MAN UNMITTELBAR BETROFFEN IST?

chnell reagieren

n Sie bemerkt haben, dass Sie Op- eines Hackerangriffs zum Beispiel in von Ransomware wurden, sollten Sie in Panik geraten. Wichtig ist es jetzt, ell zu reagieren und unverzüglich die ei zu verständigen. Für Hilfe und Infor- onen steht Ihnen auch die Meldestelle Bundeskriminalamts unter against-cy- rime@bmi.gv.at zur Verfügung.

orderungen nicht nachkommen

ngriffen in Form von Ransomware en Schadprogramme installiert, die Zugriff auf Daten und Systeme ein- schränken oder gänzlich unterbinden. Für die Freigabe der Daten werden von den Hackern oft Lösegeldforderungen gestellt. Den Forderungen der Hacker sollten Sie keinesfalls sofort nachkommen, da es nie eine Garantie dafür gibt, dass man die Daten tatsächlich wiederbekommt. Bezahlt man das Lösegeld an die Hacker, ist außerdem die Chance hoch, dass man bald wieder angegriffen wird.

! IT-Experten verständigen

Wenn Sie die Exekutive verständigt haben, sollten Sie sich umgehend an IT-Sicherheitsexperten wenden. Diese können fest- stellen, welche verbundenen Syste reits infiziert wurden und welche S als nächstes notwendig sind.
Haben Sie noch keinen IT-Security- ten? Unter www.it-safe.at werden empfohlene IT-Security-Betriebe au Österreich aufgelistet. Ersthilfe er Sie rund um die Uhr auch bei der Cy curity-Hotline der Wirtschaftkamme 0800 888 133.

© WKW

Jeder ist angreifbar

Wie einfach es ist, sich in die Server von Firmen zu hacken, weiß Martin Haunschmid, Profi- Hacker und IT-Spezialist. „In der Branche sagt man, es gibt zwei Arten von Unternehmen: Diejenigen, die gehackt wurden, und diejenigen, die noch nicht wissen, dass sie gehackt wurden", erzählt Haunschmid. „Früher oder später ist vermutlich jedes Unternehmen von Cybercrime betroffen." Als Hauptsicherheitslücken weist der Profi zwei Faktoren aus den technischen und den menschlichen Faktor. „Updates, die nicht schnell genug installiert werden, schlecht gewartete Websites, falsch konfigurierte Applikationen - das sind alles technische Lücken, die von Cyberkriminellen genutzt werden", schildert er.

„Der zweite und mindestens so wichtige Faktor ist der menschliche", so Haunschmid. Als Beispiel nennt er Phishing-Mails, die von Mitarbeitern geöffnet werden, oder das Verwenden und Weitergeben nicht sicherer Passwörter. Ein gefundenes Fressen für Hacker, so der White-Hat (Sicherheitshacker mit guten Absichten). „Solche Dinge lassen sich leicht vermeiden und zwar durchlaufende Schulungen."

Betriebsblindheit überwinden

Wesentlich in der Prävention ist zudem die Zusammenarbeit mit Profis, weiß Haunschmid. Natürlich kann man auch intern überprüfen, wo Sicherheitslücken bestehen. Hier besteht aber immer die Gefahr der Betriebsblindheit - „blind spots, die nie entdeckt und von Hackern ausgenutzt werden", erklärt er weiter. „Als beauftragter White-Hat-Hacker kann ich die Systeme eines Unternehmens, die im Internet hängen, auf Herz und Nieren testen und solche ‚blind spots' mit den Taktiken eines Cyberkriminellen ausfindig machen."

Prävention ist die beste Verteidigung

Unternehmen können viel selbst tun, um erst gar nicht Opfer einer Cyberattacke zu werden. Es beginnt mit dem achtsamen Umgang mit Nachrichten. Vor einem Klick erst nachdenken, denn ein einziger reicht aus, um enormen Schaden anzurichten. „Wenn jemand vor dem Bankomaten steht, bei dem Sie Geld abheben wollen, und sagt: ‚Grüß' Sie, ich bin Ihr persönlicher Bankberater und erleichtere Ihnen die Arbeit - geben Sie mir Ihre Karte samt Pin-Code?' Glauben Sie ihm? Oder würden Sie einem Fremden im Urlaub bedenkenlos ihr Handy geben? Wohl eher nicht. Gleiches gilt für Internet, E-Mails oder andere Nachrichten, die aufs Smartphone kommen", sagt Martin Puaschitz, Obmann der Wiener Fachgruppe UBIT. Genauso ist Betrug weit verbreitet, bei dem Betriebe beziehungsweise deren Mitarbeiter unter Verwendung falscher Identitäten zur Überweisung von Geld manipuliert werden: Sei es durch eine vermeintliche Anweisung des Geschäftsführers an die Buchhaltung oder eine Zahlungsaufforderung für einen Firmenbucheintrag. Hier ist Awareness die beste Prävention: „Alle im Betrieb müssen immer wieder daran erinnert werden, aufmerksam zu bleiben. Das ist keine einmalige Tätigkeit", so Puaschitz. Darüber hinaus sind lokale und externe Backups aller Daten wichtig. „Was nützt ein Backup auf einer Festplatte, die an meinem PC steckt? Spielt man einen Virus ein, ist auch sie betroffen", so Puaschitz. Backups müssten daher extern gespeichert und wenn möglich sogar an einem anderen Ort als im Büro aufbewahrt werden. „Im Ernstfall kann so ein Backup den Betrieb vor dem Untergang retten", sagt der Fachgruppenobmann

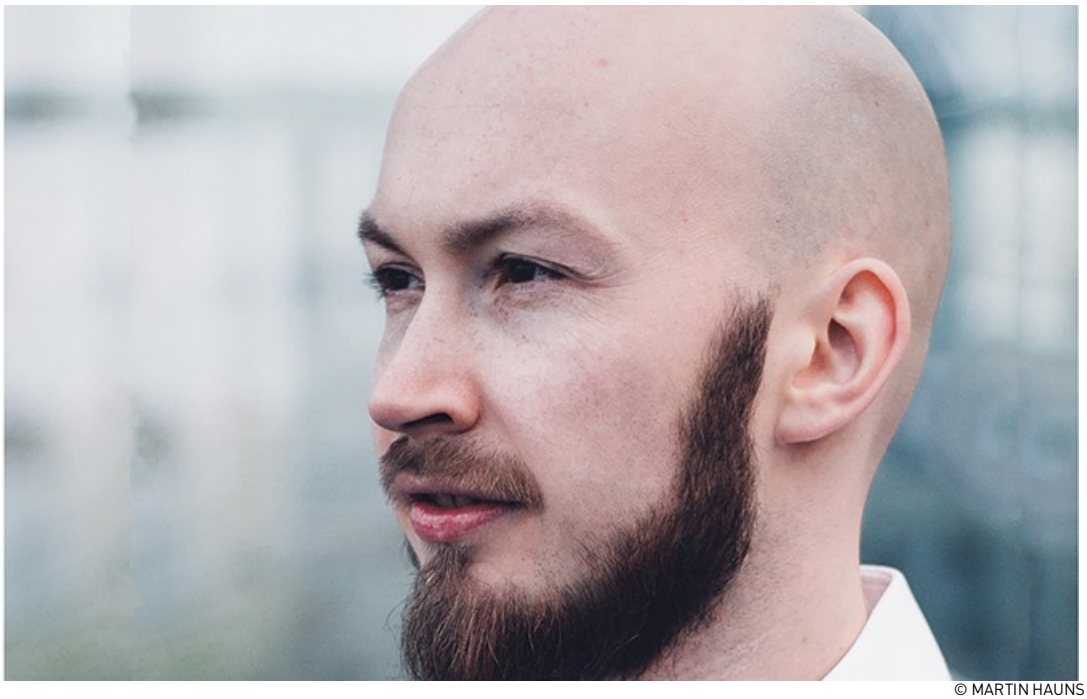
Nachgefragt!

© ATTENSAM/MARTIN STEIGER

Peter Schrattenholzer, Geschäftsführer Attensam Wien

„Niemand ist vor einem Angriff gefeit."

„Ich rate jedem Unternehmer, in Präventionsmaßnahmen zu investieren. Wir mussten am eigenen Leib erfahren, wie schnell man selbst Opfer von Cybercrime werden kann – niemand ist vor einem Angriff gefeit. Mein Tipp an alle: Technisch aufrüsten und das Personal schulen. Und: Sich früh genug einen zuverlässigen IT-Dienstleister suchen, damit man im Ernstfall schnell Unterstützung bekommt."



© MARTIN HAUNSCHMID, PROFI-HACKER

Martin Haunschmid, Profi-Hacker

„Hacker haben oft leichtes Spiel."

„Sicherheitslücken in der Technik und menschliches Versagen sind die Hauptgründe, warum Hacker bei Unternehmen oft leichtes Spiel haben. Das sind beides Faktoren, die sich durch Prävention und Awareness bei den Mitarbeitern vermeiden lassen würden. Einen 100-prozentigen Schutz vor Cyberattacken wird es nie geben, durch die richtigen Maßnahmen kann man es Cyberkriminellen aber deutlich schwerer machen.

© ARMIN HALM/BUNDESRIMINALAMT

Erhard Friessnik, Leiter Cybercrime Competence Center Bundeskriminalamt

„Ich rate Firmen zu einer Anzeige."

Unternehmen sind meist von Ransomware
betroffen - der erpresserischen Verschlüsselung von Daten. Dahinter steckt mittlerweile nicht mehr nur ein Täter, wir haben es mit organisierter Kriminalität zu tun. Angriffe sollten immer zur Anzeige gebracht werden. Serientäter verwenden oft die gleiche Vorgehensweise. Je mehr elektronische Spuren wir sicherstellen können, desto höher die Chance, die Tätergruppe zu erwischen."

© FLORIAN WIESER

Martin Heimhilcher, Spartenobmann Information & Consulting

„Fördertopf jetzt rasch aufstocken!"

Mittelunternehmen sind für die Täter angreifbarer, weil sie meist keine Ressourcen haben, um eigene IT-Security Abteilungen einzurichten. Es braucht mehr Fördermittel für Cybersicherheit. Der Fördertopf des aws, der am 1. April startete, ist bereits ausgeschöpft. Die große Nachfrage zeigt, dass er unbedingt aufgestockt werden muss."

Das könnte Sie auch interessieren

Positive Bilanz zum 1. Einkaufssamstag im Wiener Handel

Handelsobfrau Gumprecht: „Umsatzstärkste Zeit des Handels ist eingeläutet" - 1,4 Millionen Wiener wollen Geschenke kaufen - Renner am 1. Einkaufssamstag: Adventkalender, Spiel- und Parfümwaren, Bekleidung › mehr

Wien tanzt wieder

Saisoneröffnung der Tanzschulen –Tag der offenen Tür in den 24 Wiener Tanzschulen am Sonntag, 18. September – Wiener Tanzprofis bieten vielfältiges Kursprogramm › mehr

25 Prozent verschenken zu Weihnachten Bücher

Glöckler: "Kaufen Sie beim Buchhändler Ihres Vertrauens." - Frauen lesen anders; Männer auch

› mehr