IT-Sicherheit: Hacker im Heimbüro

Bozen – Der viel gepriesene Digitalisierungsschub der vergangenen Monate hat erneut gezeigt, wie wichtig Datenschutz und Datensicherheit sind. Allein die Zugriffe auf Unternehmensressourcen aus dem Homeoffice bereitzustellen, war eine riesige Herausforderung für viele Unternehmen. Die erforderliche Cybersecurity blieb angesichts möglichst pragmatischer Lösungen oft auf der Strecke. Dabei gilt der Grundsatz: Mehr Homeoffice verlangt auch mehr IT-Sicherheit. Internetkriminelle wissen um die Lücken und versuchen die Gunst der Stunde zu nutzen. Mit Spam, Phishing, Malware, Identitätsdiebstahl und Datenklau wollen sie schnelle Beute machen. Das europäische Polizeiamt Europol stellte vor Kurzem fest, dass die Auswirkungen der Coronakrise in keinem anderen Deliktsfeld so gravierend sind wie im Bereich Cybercrime. In Südtirol hat es indes noch keinen Anstieg der gemeldeten Straftaten gegeben. „Die Situation ist weiterhin überhaupt nicht besorgniserregend", beruhigt Ivo Plotegher, Stellvertretender Kommissar der Staatspolizei und Leiter der Polizeidienststelle für Post- und Kommunikationswesen in Bozen.

Dass auch hierzulande die Verwundbarkeit vieler Unternehmen vor allem durch unzureichend abgesicherte Homeoffice-Verfahren gestiegen ist, bestätigt Peter Nagler, Direktor des IT-Dienstleisters Konverto. Im Interview erklärt er, wie sie sich schützen können.

SWZ: Herr Nagler, welches sind die größten IT-Sicherheitsrisiken, wenn von zuhause gearbeitet wird

Peter Nagler (Foto: Konverto)

Peter Nagler: Grundsätzlich ist es so, dass immer ein Restrisiko besteht, wenn ein Gerät nicht durch das Unternehmen abgesichert ist, zum Beispiel wenn ein privates Gerät zuhause von mehreren Personen benutzt wird. Das kann ein Familien-PC sein, also ein Springergerät, auf das sensible Daten geladen werden, Dateien der Firma, die lokal abgespeichert werden, um besser arbeiten zu können. Wenn andere Personen als der Mitarbeiter bzw. die Mitarbeiterin damit arbeiten, können sie mitunter ungewollt sensible oder firmeninterne Daten für Dritte zugänglich machen.

Zugleich wissen Hacker*innen, dass derzeit viel von zuhause gearbeitet wird und richten ihre Tätigkeit dementsprechend aus bzw. nutzen andere Wege. Man sieht immer mehr, dass Angreifer*innen auf freundschaftliche Art versuchen, Zugriff zu erhalten.

Können Sie konkrete Beispiele nennen?

Phishing-Mails etwa, die zuhause schwieriger zu erkennen sind. Es fehlt die Rücksprachemöglichkeit mit Kolleg*innen, wenn man sich unsicher ist, klickt man vielleicht eher. Eine beliebte Masche ist auch, über Chatprogramme einzudringen oder sogar potenzielle Opfer direkt über diese virtuellen Kanäle anzurufen. Der Angreifer bzw. die Angreiferin gibt sich als IT-

Mitarbeiter*in der Firma aus oder als jemand, der in ihrem Auftrag handelt, und verlangt Zugriff, zum Beispiel über TeamViewer, auf den PC oder Laptop, um ein angebliches Problem zu beheben oder eine Einstellung zu kontrollieren. Das sind keine theoretischen Fälle, sondern so tatsächlich in Südtirol passiert. Vonseiten der Hacker*innen sind das natürlich gewagte Aktionen, die entlarvt werden könnten, dennoch scheinen sie zu funktionieren.

Es ist folglich einmal mehr der Mensch die Schwachstelle, die Angriffe ermöglicht?

Beim Phishing wird prinzipiell immer die Gutmütigkeit bzw. Gutgläubigkeit des Menschen ausgenutzt. Die Hacker*innen gehen dabei immer professioneller vor. Sie schicken per Mail oder Chat einen Link, auf den man klicken soll, man landet auf einer Website mit vorausgefülltem Formular mit Namen, E-Mail-Adresse usw. Das weckt zusätzliches Vertrauen.

Sogar digitale Zertifikate werden gefälscht, wodurch zum Beispiel eine gefakte Teams-Einladung von mir geöffnet werden kann, ohne dass ich eine Warnung erhalte.

Vorhin haben Sie bereits erwähnt, dass die Nutzung privater Endgeräte riskant sein kann. Was genau gilt es da zu beachten?

Wichtig ist auf jeden Fall, eine professionelle Antivirensoftware zu verwenden, die ständig aktualisiert wird. Rechtlich sind Arbeitgeber*innen sogar dazu verpflichtet, derartige Software für die Arbeitszeit bereitzustellen. Der Gesetzgeber unterscheidet dabei eigentlich nicht zwischen Arbeit im Büro oder betriebliche Verwendung zuhause.

Außerdem sollte ein Unternehmen sicherstellen, dass keine Daten auf den privaten PC heruntergeladen werden. Das ist nicht einfach, aber grundsätzlich möglich und gelingt etwa über den Zugriff auf einen virtuellen Desktop. Auf diese Art hinterlasse ich keine Spuren auf meinem Heim-PC, und im Falle eines Diebstahls des Gerätes habe ich keine Probleme mit verlorenen Daten – wobei ich ohnehin jedem raten würde, eine Festplattenverschlüsselung einzusetzen. Dank Zugriff auf einen virtuellen Desktop verwende ich meinen Heim-PC jedenfalls praktisch nur, um darzustellen, was auf meinem Büro-PC zu sehen ist.

Eine sehr sichere Methode der Anmeldung von zuhause oder unterwegs erfolgt heutzutage über eine Multifaktor Authentisierung (MFA), das bedeutet, dass ich immer zwei Wege nutze, z. B. eben den Laptop und mein Smartphone.

Außer ein*e Mitarbeiter*in lädt sich nichtsdestotrotz Dateien herunter, weil die Verbindung zu langsam ist, weil es bequemer erscheint oder Ähnliches. Kann auch das verhindert werden?

Der Administrator kann festlegen, ob Dateien heruntergeladen werden können. Allerdings ist eine solche Festlegung auf Dateiebene mit großem Aufwand verbunden. Besser wäre die Festlegung auf Ebene der Firewall, wo der Zugriff erfolgt. Idealerweise stellt das Unternehmen auch eine Firewall am Heimarbeitsplatz zur Verfügung, die es managt. So kann ein sicheres Virtual Private Network (VPN, Anm. d. Red.) eingerichtet werden.

Der Einsatz von VPN gilt als klassischer Weg. Was ist der Unterschied zu einer Remote Access Solution (RAS) wie TeamViewer?

TeamViewer ist nicht unbedingt die Lösung, die empfohlen wird, da dem Programm praktisch alle Ausführrechte auf dem PC eingeräumt werden. VPN ermöglicht einen Zugriff aufs Firmennetz, es ist wie eine Art Tunnel von Punkt zu Punkt, ein virtueller Kabel von meinem Heim-PC zur Firewall in der Firma, über die ich definieren kann, was der Zugreifende tun darf – und was nicht. VPN ist daher eine sehr sichere Lösung, insbesondere wenn die Firewall des privaten Geräts von der Firma gemanagt wird.

Haben Sie weitere Tipps für Unternehmen?

Ich würde einen Dreischritt empfehlen, wobei professionelle Beratung das A und O ist: Gemeinsam mit einem Experten können Unternehmer*innen in einem ersten Schritt erheben, was ihre individuellen Anforderungen sind. Ein Architekturbüro, das mit sehr großen Dateien arbeitet, wird andere haben als eine Buchhaltung. In einem zweiten Schritt wird darauf

aufbauend ein Konzept erstellt, das umgesetzt und im Idealfall – drittens – periodisch von externen Sicherheitsunternehmen überprüft und aktualisiert wird.

Sollten sprachgesteuerte Geräte ausgeschaltet und Webcams im Homeoffice abgedeckt werden, oder wäre das übertriebene Vorsicht?

Übertrieben ist es nicht. Es gibt leider immer neue Programme, die auf die Webcam zugreifen, ohne dass das Lämpchen leuchtet. Die Kamera kann ich mit einer Abdeckblende oder auch einem Stück Klebestreifen physisch abdecken, beim Mikrofon ist es schwierig. Hier kann man nur raten, erstens das Betriebssystem immer auf dem aktuellsten Stand zu halten, ebenso wie, zweitens, wesentliche Audio- und Videotreiber.

Das Thema Cybersecurity wird nach wie vor von manchen Unternehmen stiefmütterlich behandelt. Was spricht dafür, sich damit auseinanderzusetzen?

Die IT-Sicherheit ist heute ein wesentlicher Faktor, um das Überleben des Unternehmens zu sichern. Ohne Schutz kann mein ganzes Firmennetzwerk gestört werden. Wenn ich anschließend mehrere Tage nicht arbeiten kann, ist das ein enormer Schaden.

Interview: Sabina Drescher

Edition: 40-20