Blue Shield schützt Unternehmen zuverlässig vor Cyberkriminalität

Die Gefahren aus dem Netz nehmen rasant zu, Angriffe werden immer hinterhältiger. Wer jetzt nicht reagiert, läuft Gefahr ins Netz der Cyberkriminellen zu geraten und muss mit großem wirtschaftlichen Schaden rechnen.

Die Internetkriminalität steigt mit zunehmender Digitalisierung unserer Gesellschaft in besorgniserregendem Ausmaß an. Der Cybercrime-Report 2020 des Innenministeriums nennt alarmierende Zahlen: So sind Angriffe auf Daten oder Computersysteme gegenüber 2019 gleich um 69,4% gestiegen. Nicht nur die Anzahl von 12.914 angezeigten Delikten im Jahr 2020, das entspricht rund 35 Fällen pro Tag, sondern auch die immer noch täuschend echter wirkenden Methoden der Hacker geben zu bedenken.

BILD: SN/WAU-EFFEKT/CELIA RITZBERGER

Unternehmensgründer Alois Kobler (l.) und Cyber-Security-Experte Avi Kravitz (r.) von Blue Shield Security aus Oberösterreich sagen Cyberkriminalität den Kampf an.

Hacker-Angriff: Wenn plötzlich nichts mehr geht

Bedeutende, international tätige Unternehmen in Salzburg, aber auch in Oberösterreich und anderen Bundesländern waren bereits betroffen und mussten schmerzvoll die bittere Erfahrung groß-angelegter Hacker-Attacken spüren. Ob groß oder klein, treffen kann es jeden. Die Daten sind plötzlich verschlüsselt, der Bildschirm steht still, nichts geht mehr, Lösegeld wird gefordert. Ein Alptraum für jedes Unternehmen, egal welcher Branche und Größe. Wer sich schützen will sollte lieber schon gestern als morgen, präventive Vorkehrungen treffen.

Blue Shield schützt zuverlässig

Eine zuverlässige Lösung bietet das in Oberösterreich ansässige Unternehmen Blue Shield Security. Das auf Cybersecurity spezialisierte Unternehmen hat ein weltweit einzigartiges IT-Produkt entwickelt, das vor Hackerangriffen schützt und setzt damit Maßstäbe in der europäischen IT-Sicherheitsbranche. Dabei handelt es sich um eine cloudbasierte Software namens Blue Shield Umbrella, die auf Basis künstlicher Intelligenz Bedrohungen bereits vor dem Eindringen in das Netzwerk abwehrt.

Auch bisher noch unbekannte Angriffe verhindert die Software. Während andere IT-Sicherheitslösungen meist mit einem Denylist-basierten Ansatz arbeiten, der voraussetzt, dass der Schädling bereits bekannt ist, verfolgt Blue Shield einen gänzlich anderen Weg: Der viel strengere Allowlist-basierte Filter qualifiziert bereits im Vorhinein angefragte Domänen, lässt die Schadsoftware erst gar nicht ins System und schließt somit ein Infektionsrisiko von vornherein aus. In Ergänzung auch zu bereits bestehenden Sicherheitssystemen lässt sich Blue Shield Umbrella problemlos innerhalb von 15 Minuten einrichten. Mit der Software bietet das Unternehmen eine österreichische Lösung, bei der sämtliche Daten in heimischen Rechenzentren gesichert werden.

IT-Sicherheit auf Wirksamkeit überprüfen

Die Vorgangsweisen der Cyberkriminellen werden immer noch trickreicher. Sie versenden täuschend echt aussehende E-Mails mit Schadsoftware an Firmen, legen deren IT-Systeme lahm und fordern teures Lösegeld für die Freigabe der Daten. Der wirtschaftliche Schaden ist enorm. „Spätestens jetzt sollten Unternehmen ihre IT-Sicherheitssysteme auf ihre Wirksamkeit überprüfen. Das beste Backup-Konzept bringt nichts, wenn dieses nicht laufend auf seine Wirksamkeit getestet wird", rät Cyber-Security-Experte Avi Kravitz von der Firma Blue Shield Security.

Betrug mit geklauter Identität

Die größten, sichtbaren Gefahren für Unternehmen sieht Kravitz aktuell in mehreren Bereichen: Mit dem sogenannten „Business-E-Mail-Compromise", auch als „CEO Fraud" bekannt, verschaffen sich Hacker illegal Zugriff auf geschäftliche E-Mail-Konten. Dabei ist das erste Ziel der Betrüger sich Zugriff auf die Mailbox ihrer Opfer zu verschaffen. Dies geschieht meistens über Phishing-Links, mit Hilfe derer Passwörter „abgefischt" werden oder über geleakte, also ungewollt veröffentlichte Passwörter von gehackten Web-Portalen.

Erpressung mit verschlüsselten Daten

Eine zunehmende Bedrohung ist auch die als Erpressersoftware bekannte Ransomware. Das sind Schadprogramme, welche das Ziel haben, alle Computer sowie Datenablagen zu verschlüsseln, um so Geld für die Entschlüsselung zu erpressen. Ransomware dringt vor allem durch verseuchte E-Mail-Attachments, veraltete Software oder unzureichend gesicherte Netzzugänge ein und richtet bei betroffenen Organisationen enormen Schaden an. Statistiken zu Folge braucht ein Unternehmen, selbst wenn es bezahlt hat, noch drei Wochen um die Systeme wiederherzustellen.

BILD: SN/ADOBE STOCK/NICOELNINO

Supergau: Angriff auf die Lieferkette

Die dritte zunehmende große und verhängnisvolle Gefahr sieht Kravitz in den sogenannten Supply Chain Angriffen, bei denen nicht nur das direkt attackierte Unternehmen kompromittiert wird, sondern auch deren Kunden und Kundeskunden zu Opfern werden. Einer der kriminellsten Hackerangriffe dieser Art ereignete sich 2020 auf das US-Unternehmen SolarWinds. Der Softwarehersteller SolarWinds wurde gehackt und mit ihm in der Folge weltweit rund 18.000 Kunden infiziert, darunter staatliche Organisationen, europäische Behörden und IT-Größen wie Microsoft, Cisco, Intel sowie viele andere.

Gehackt werden nur die anderen?

Betreffen Angriffe dieser Art nur die Großen und ist eine Bedrohung so weit weg? Leider nein, denn auch in Oberösterreich gab es erst im September dieses Jahres einen Supply Chain Angriff auf ein Unternehmen, bei dem in der Folge über 30 Unternehmen davon betroffen waren. Bedingt durch die erfolgreiche Attacke auf einen EDV-Dienstleister, gelang es den Hackern sich Zugriff zu Kunden des Dienstleisters zu verschaffen. Dieser Angriff gilt als die bisher größte Cyber-Attacke Österreichs. Die betroffenen Unternehmen waren mit hohen Lösegeldforderungen konfrontiert.

Einzigartiger Schutz mit Blue Shield Umbrella

Alle Experten sind sich einig, die explosionsartige Zunahme an Cyberkriminalität erfordert jedenfalls die Berücksichtigung von IT-Sicherheit als oberste Priorität auf allen Ebenen. Nur so kann sichergestellt werden, dass auch systemrelevante Strukturen weiterhin reibungslos funktionieren. Blue Shield Umbrella schützt vor akuten Bedrohungen wie Phishing, bei dem sensible Daten mit gefälschten Mails ergaunert werden, Ransomware (Erpressersoftware) oder komplett neuen Bedrohungen (sogenannte Zero-Days). Für den weltweit einzigartigen Schutz, der selbst über Machine Learning und künstliche Intelligenz verfügt, erhielt das Unternehmen aus Oberösterreich bereits mehrfach Auszeichnungen.

Über Blue Shield Security

Blue Shield Security wurde 2015 in Oberösterreich gegründet und schützt Unternehmen und Organisationen vor Cyberkriminalität. Die Firmenzentrale mit über 30 Beschäftigen im Bereich Forschung und Entwicklung befindet sich in Leonding bei Linz.

Der in Österreich entwickelte Blue Shield Umbrella ist ein cloudbasiertes System und der weltweit einzige Allowlist Filter auf Basis künstlicher Intelligenz. Blue Shield Security bietet einen zuverlässigen, vorausschauenden und selbstlernenden Schutz vor neuen Bedrohungen.

Schadhafte Webseiten und E-Mails werden bereits vor Eindringen in das Netzwerk gefiltert und blockiert, wodurch Unternehmen zuverlässig vor akuten Bedrohungen geschützt sind. Sämtliche Daten werden dabei in Österreich – in heimischen Rechenzentren – gesichert.

Die Mitarbeiterinnen und Mitarbeiter der Firma Blue Shield in Österreich sind vor Ort erreichbar. Unter dem Schutz des Blue Shield Umbrella's stehen bereits Krankenhäuser, Behörden, Ministerien, Energieversorger, Bahnen und andere Top-Arbeitgeber Österreichs.

Kontakt:
Blue Shield Security
Kornstraße 7a
A-4060 Leonding
Tel.: +43 732/211922
E-Mail: OFFICE@BLUE-SHIELD.AT
WWW.BLUE-SHIELD.AT

BlueShield

Fünf Tipps für mehr Cybersicherheit im Unternehmen:

1) IT-Sicherheitssysteme regelmäßig auf die Wirksamkeit überprüfen und anpassen inklusive der Backup- & Wiederherstellungsprozesse
2) Software stets auf dem aktuellen Stand halten
3) Cybersecurity-Beauftragten einsetzen
4) Cybersecurity ist keine einmalige Aktion, sondern ein Prozess.
   Daher: regelmäßige Wirksamkeitsprüfungen / Security Checks!
5) Multi-Faktor-Authentifizierung für alle Nutzerkonten einrichten