

Cyber-Security Studie zeigt: 30% der Salzburger Unternehmen sind leicht angreifbar

Knapp jedes dritte Unternehmen im Bundesland Salzburg betreibt Server-Systeme mit kritischen Sicherheitslücken.

Im Mai 2020 wurde für ca. **52.000 österreichische Unternehmen**, die aufgeteilt nach Bundesland/Bezirk und Branche aus öffentlichen Quellen bezogen wurden, eine sogenannte **OSINT-Studie** durchgeführt. OSINT steht für **Open Source Intelligence** und bedeutet, dass Informationen aus frei verfügbaren, offenen Quellen verwendet werden. Ziel war es herauszufinden, wie Unternehmen mit bereits - teilweise länger - **bekanntem Sicherheitslücken** in ihrer **öffentlich erreichbaren IT-Infrastruktur** umgehen und sich vor Hackerangriffen schützen. Erste **Ergebnisse dieser Studie** zeigen, dass bei einem überraschend großen Anteil der Unternehmen (nicht gepatchte) und daher bekannte IT-Sicherheits-Schwachstellen vorliegen, die Hacker für Angriffe, Datendiebstahl oder ähnliches leicht nutzen können.

“In Zeiten von Corona und Home-Office sind das leider keine guten Nachrichten. **Bekannte IT-Sicherheitsschwachstellen** die älter als 1 Jahr sind, sind **verantwortlich für einen überwiegenden Großteil (90%)** der erfolgreich durchgeführten **Cyber-Angriffe auf IT-Infrastruktur.**“, so Martin Herfurt, der Studienautor.

Die unschönen **Konsequenzen** von Cyber-Angriffen sind bekannt: Es kommt zu **Datenleaks, Systemausfällen** und zur **kriminellen Verwendung von betroffenen Systemen**. Das hat zur Folge, dass auf diese Weise kompromittierte Unternehmen ihr **erarbeitetes Know-How** an Mitbewerber*innen verlieren. Ihre **Reputation** leidet und sie haben infolge solcher Angriffe mit **wirtschaftlichen Konsequenzen** zu rechnen.

Prominentes Beispiel: Das US-Amerikanische Unternehmen GARMIN erlitt erst kürzlich einen Ransomware-Angriff, bei dem großer wirtschaftlicher Schaden und der Verlust von Reputation die Folge waren. Kolportiert wird, dass GARMIN eine zweistellige Millionensumme an “Lösegeld” zahlen musste. Zur Erklärung: Ransomware sind Schadprogramme, die Computer sperren oder darauf befindliche Daten verschlüsseln. Die Täter erpressen ihre Opfer, indem sie deutlich machen, dass sie die Daten nur nach einer Lösegeldzahlung wieder freigegeben werden.

86,2% der auf Salzburger Server-Infrastruktur identifizierten Schwachstellen sind **älter als 2 Jahre** und somit mit hoher Wahrscheinlichkeit mit bereits verfügbaren Hacker-Tools angreifbar.

Der Bezirk **St. Johann im Pongau** ist - mit einem Mittelwert von **4,22 Schwachstellen pro Server** - der am stärksten von Security-Schwachstellen betroffene Bezirk.

Hinter der Studie steht ein innovatives Salzburger Start-up, das sich auf IT-Risikoabschätzungen und IT-Security spezialisiert hat. Als Experte für Applikations-Sicherheit hilft der “IT-Wachdienst” großen und kleinen Unternehmen dabei rasch und effizient ihr IT-Security Risiko zu minimieren. So bietet “IT-Wachdienst” – neben **IT-Sicherheitsberatung** und **Sicherheitsüberprüfungen** - auch regelmäßig durchgeführte **Schwachstellen-Scans** für Unternehmen an.

Autor der Studie:

DI(FH) Martin Herfurt ist geschäftsführender Gesellschafter der “toothR new media GmbH” mit Sitz im Land Salzburg. Seit etwa 20 Jahren befasst sich er intensiv mit dem Thema IT-Sicherheit. Unter anderem ermöglichte ihm die frühe, einschlägige Arbeit im Bereich Bluetooth Sicherheit und die daraus folgende Zusammenarbeit mit der Bluetooth SIG – dem Standardisierungskörper für den Bluetooth Standard – zahlreiche Vorträge auf internationalen IT-Sicherheitskonferenzen.

Nach mehrjähriger Tätigkeit als IT-Sicherheitsberater und Penetrationstester, kooperiert Martin Herfurt seit 2014 mit dem deutschen Unternehmen “Greenbone Networks GmbH,” welches den Unternehmensfokus im Bereich professionellen Schwachstellen-Managements hat.

Mehr dazu: https://www.it-wachdienst.com/press/osint-2020_vulnerability_studie_salzburg/