Cyber-Security Studie zeigt: Viele Unternehmen in der Steiermark haben Nachholbedarf beim Thema IT-Sicherheit

29% der Unternehmen im Bundesland Steiermark 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 **O**pen **S**ource **Int**elligence und bedeutet, dass Informationen aus frei verfügbaren, offenen Quellen verwendet werden. Ziel war es herauszufinden, wie Unternehmen mit bereits - teilweise länger - **bekannten 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 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

85,69% der auf Steirer Server-Infrastruktur identifizierten Schwachstellen **sind älter als 2 Jahre**. Im Bezirk **Südoststeiermark** liegt der Anteil der Schwachstellen mit einem Alter von zwei und mehr Jahren bei **90,51%**.

Der **Bezirk Gröbming** fällt mit einer für das Bundesland Steiermark **überdurchschnittlich hohen Schwachstellen-Belastung pro Server (3.41)** besonders auf.

Die mittlere **Schwachstellen-Belastung pro Unternehmen** ist im **Bezirk Leoben mit 20,88 gut doppelt so hoch** wie im gesamten Bundesland Steiermark.

Sehr kleine Unternehmen (in dieser Studie sind das Unternehmen mit nur einem Server) sind mit einem Mittelwert von **21,92 Schwachstellen pro Server** bzw. Unternehmen die am stärksten mit Schwachstellen belastete Unternehmensklasse.

Hinter der Studie steht ein innovatives Salzburger Start-up, dass 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 sich 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/blog/osint-2020-steiermark/