1. Cyber-Security-Studie Österreichs bringt spannende Ergebnisse

Unternehmen und Einrichtungen haben starken Nachholbedarf – Betroffene können Check-Protokoll anfordern

Heute Mittwoch, 7. Oktober 2020 präsentierte das Salzburger Start-Up Unternehmen „IT-Wachdienst" erstmals für Österreich eine umfassende IT-Cyber-Security-Studie, bei der über 50.000 Unternehmen, Hochschulen, Ministerien oder Behörden und deren Internet-Domains auf kritische Sicherheitslücken überprüft wurden. Die Analyse der Ergebnisse zeigt, dass viele starken Nachholbedarf im Bereich der IT-Sicherheit haben. Immerhin mehr als 22% der getesteten Einrichtungen weisen hochkritische Sicherheitslücken, nach der objektiven und bewährten CVSS-Metrik[1] auf.

„Das Ziel dieser Studie war es, den Ist-Zustand von Unternehmen in Bezug auf deren IT-Schwachstellen-Management bzw. der Cyber-Resilienz ihrer IT-Infrastruktur zu ermitteln", so Martin Herfurt und weiter: „Der Trend zu Home-Office-Arbeitsplätzen zwingt viele Unternehmen in die Öffnung zum Internet. Diese Vergrößerung von öffentlich erreichbarer Angriffsoberfläche bedingt einen höheren Aufwand für die Wartung kritischer IT-Systeme - eine Tatsache, die viele Unternehmen zu unterschätzen scheinen."

Viele Filme und Romane (z.B. Blackout von Marc Elsberg) beschäftigen sich mit den Auswirkungen von Hackerangriffen auf die IT-Infrastrukturen von Firmen oder Ländern und sie zeigen, wie umfassend die negativen Effekte von erfolgreichen Cyberattacken sein können. Erst kürzlich wurde das US-Amerikanische Unternehmen GARMIN Opfer eines sogenannten 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, um wieder Zugriff auf die eigenen Daten zu bekommen. Martin Herfurt, der Autor der Studie verfügt über mehr als 20 Jahre Erfahrung im Bereich der IT-Security, aber die Ergebnisse haben selbst den Experten überrascht.

[1] Common Vulnerability Scoring System (wörtlich übersetzt: Allgemeines Schwachstellenbewertungssystem), abgekürzt CVSS, ist ein Industriestandard zur Bewertung des Schweregrades von möglichen oder tatsächlichen Sicherheitslücken in Computer-Systemen. Im CVSS werden Sicherheitslücken nach verschiedenen Kriterien, sogenannten Metrics, bewertet und miteinander verglichen, so dass eine Prioritätenliste für Gegenmaßnahmen erstellt werden kann

Detailergebnisse der Studie:

- Auf Grund der vorliegenden Daten ist Tirol mit 35,6% Unternehmen mit kritischen Sicherheitsmängeln das unsicherste Bundesland. Knapp gefolgt von Wien (31,24%) und Salzburg (30,07%).
- Im öffentlichen Bereich ergibt sich ein ähnliches Bild: 37,22% der gescannten Einrichtungen haben hohe kritische Schwachstellen. Ein Ergebnis sticht hier besonders ins Auge: 57,16% der Ministerien sind durch kritische Schwachstellen prinzipiell für Hacker*innen leicht angreifbar.
- Von der Typographie der entdeckten Schwachstellen sind 27,65% vom Typ „Denial of Service" (DoS = Nichtverfügbarkeit eines Internetdienstes). Auf Platz zwei liegt mit 15,16% eine Schwachstellentyp mit dem Titel „Overflow". Das ist ein Pufferüberlauf, der dazu führt, dass Angriffe ausgeführt werden können, die eine Eskalation von Berechtigungen bewirken und somit einen uneingeschränkten Zugriff auf Rechner ermöglichen können. Der berühmte Morris-Wurm 1988 verwendete dies als eine seiner Angriffstechniken. Nummer drei auf der Liste der Schwachstellen nimmt mit 9,72% die „Code Execution" ein. Die Remote-Code-Ausführung (Code Execution) stellt die Möglichkeit eines Angreifers dar, aus der Ferne auf Computer und Endgeräte zuzugreifen und dort Änderungen durchzuführen oder Programme und Software auszuführen.
- Sieht man sich die Schwachstellen pro Unternehmen an, so ist das gefährdendste Bundesland ebenso Tirol, mit 11,28 Schwachstellen pro geprüften Unternehmen.
- Auf Bezirksebene ist der Lungau (S) mit 49,06% hohen Risiko der unsicherste Bezirk Österreichs. In absoluten Zahlen gibt es im Bezirk Kufstein (T) mit 11.678 die meisten Schachstellen.
- Im öffentlichen Bereich gibt es auch interessante Erkenntnisse: 57,24% der Schwachstellen in den überprüften Ministerien sind bereits älter als sechs Jahre . Während bei Hochschulen, Behörden und Kliniken nur knapp 18 – 25% älter als sechs Jahre sind. Dafür sind in diesen drei Bereichen die meisten Schachstellen (61-68%) zwischen zwei und sechs Jahre alt. Auch das sind für Experten sehr kritische Werte.
- Nach Sparten aufgegliedert ergibt sich folgendes Bild: In der Sparte „Industrie" liegt mit 37,82% das Sicherheits-Risiko am höchsten. Gefolgt von den Sparten „Transport" und „Verkehr" (31,02%) und Banken und Versicherungen (31,01%). Somit ist laut Ansicht der Experten kritische Infrastruktur in Österreich nicht besonders gut geschützt.
- 22,16% der identifizierten Schwachstellen sind aufgrund ihrer CVSS-Bewertung als hochkritisch, 70,19% als mittelkritisch und 7,66% als Schwachstellen mit niedriger Kritikalität einzuordnen.

- Nach Stichprobengröße[2] ergibt sich folgendes Bild: Je größer und breiter der Internetauftritt und das Serviceangebot, umso höher die Sicherheitsrisiken. Groß heißt 15-30 IP-Adressen und hier ergibt sich eine erhebliches Sicherheitsrisiko von über 83%. Sehr kleine Unternehmen (mit einem Server) fallen durch eine hohe Schwachstellenbelastung pro Asset auf, wobei große Unternehmen (mit vielen Servern) mit einer hohen Schwachstellen-Belastung pro Unternehmen auffallen.

Für den Verfasser der Studie scheint es so, als ob Sicherheit der IT-Infrastruktur in Österreich immer noch ein wenig stiefmütterlich behandelt wird. Vielen Unternehmen, aber auch dem öffentlichen Bereich verhalten sich so, als ob Hacker-Angriffe sie nicht treffen können und das obwohl der Bereich Cybercrime im Jahr 2019 knapp 28.500 Straftaten - laut der Statistik des BKA`s - zugeordnet werden. Das ist ein Plus von knapp 45% im Vergleich zum Vorjahr, so Martin Herfurt. Der Experte verweist gleichzeitig, dass die Aufklärungsquote im Bereich des Cybercrimes leicht sinkt und empfiehlt mehr in die IT-Sicherheit zu investieren, denn jeder Euro rechnet sich. Nach einem Angriff ist es oftmals zu spät und der Schaden groß. Dieser kann in die Millionenhöhe gehen. Unter Cybercrime versteht man üblicherweise alle Straftaten, die unter Ausnutzung der Informations- und Kommunikationstechnik (IKT) oder gegen diese begangen werden. Im engeren Sinne umfasst es jene Straftaten, bei denen Angriffe auf Daten oder Computersysteme unter Ausnutzung der Informations- und Kommunikationstechnik begangen werden (zum Beispiel Datenbeschädigung, Hacking, DDoS - Attacken).

Aus Sicht der Experten der Studie gibt es folgende erste Fazits aus den Ergebnissen:

- Der Nachweis von bekannten Sicherheits-Schwachstellen auf öffentlich erreichbaren Servern ist ein Gradmesser für den Umgang der jeweiligen Unternehmen mit dem Thema IT-Sicherheit.
- Viele IT-Sicherheits-Studien belegen, dass die Ausnutzung bekannter Sicherheitsschwachstellen, die älter als ein Jahr sind, verantwortlich für über 90% der erfolgreich auf Server-Infrastruktur durchgeführten Angriffe. Daher lässt sich klar aussagen, dass Österreich auf Grund der Ergebnisse erheblichen Nachholbedarf im Bereich der IT-Secruity hat. Man könnte fast sagen im Bereich der IT-Sicherheit ist Österreich ein „Entwicklungsland".
- Eine Kette ist nur so stark wie ihr schwächstes Glied: Eine einzige Schwachstelle reicht oftmals aus, um ein Unternehmen zu kompromittieren.
- Ist der Angriff auf ein Server-System erfolgreich, so kann - je nach exponierter Schwachstelle - die Verfügbarkeit, die Vertraulichkeit und/oder die Integrität der

[2] Gliederung siehe Klassifizierung der Unternehmen nach Anzahl der Assets

jeweiligen Infrastruktur und deren Daten nicht mehr gewährleistet werden. Mit anderen Worten: 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 verlieren. Ihre Reputation leidet und sie haben infolge solcher Angriffe mit wirtschaftlichen Konsequenzen zu rechnen.

- Die hier verwendete quantitative Untersuchungsmethode unter Zuhilfenahme öffentlicher Daten erlaubt Aussagen über die Gesamtsituation vieler Unternehmen. Diese Methode wird ebenfalls von Cyberkriminellen verwendet, um Ziele für Angriffe zu identifizieren.
- Im Einzelfall empfehlen die Expertinnen und Experten, regelmäßige Durchführung (Sicherheits-Audits) von Schwachstellenscans auf die gesamte IT-Infrastruktur und die gezielte Überprüfung von Anwendungen, die mit besonders sensiblen Daten zu tun haben und/oder individuell für eine kleine Benutzerzahl entwickelt wurden. Mit Hilfe von definierten Prozessen kann die Cyber-Resilienz langfristig auf einem konstanten Level gehalten werden.

Trotz der öffentlichen Verfügbarkeit der in dieser Studie verarbeiteten Daten stellt die Veröffentlichung dieser Daten als Zusammenstellung ein zusätzliches Risiko für die betroffenen Unternehmen dar. Unternehmen können via E-Mail an studie-oesterreich@it-wachdienst.com Information zu der jeweiligen Absender-Domain der E-Mail anfordern.

Für das Jahr 2022 ist bereits eine Wiederholung der Studie angedacht. „Das Thema Cyber-Sicherheit wird uns weiterhin beschäftigen. Wir vermuten, dass die Dunkelziffer der erfolgreichen Angriffe, trotz der Meldepflicht, viel höher ist, als die bekannten Einzelfälle. Wer gibt schon öffentlich gerne zu, dass sein Unternehmen etc. Opfer einer Cyber-Attacke geworden ist. Vielleicht können wir mit dieser Erhebung ein Umdenken einleiten, denn nur gemeinsam können wir Österreich auch im Internet sicherer machen!" so Martin Herfurt abschließend.

Über den Autor

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.

Wer ist der IT-Wachdienst?

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.

Über die Studie:

- Das Ziel dieser Studie war es, den Ist-Zustand von Unternehmen in Bezug auf deren IT-Schwachstellen-Management bzw. der Cyber-Resilienz ihrer IT-Infrastruktur zu ermitteln.
- Die Stichprobengröße in Österreich sind 50.537 Unternehmen und 634 öffentliche Einrichtungen, wie Hochschulen, Ministerien Kliniken und/oder Behörden.
- Erhebungszeitraum war Mai (Unternehmen) und Juni (öffentlicher Bereich) 2020.
- Die Datenbasis für diese Studie stammt aus einer öffentlichen Datenbank der Wirtschaftskammern Österreichs. Segmentiert nach Sparte und Bundesland wurden hier diejenigen Unternehmen selektiert, welche mit einer Internetdomain in Verbindung gebracht werden konnten.
- Die Analyse der mit der jeweiligen Internetdomain in Verbindung stehenden Server-Systeme wurde passiv (ohne direkten Zugriff auf diese Systeme) und mit öffentlich verfügbaren Informationen durchgeführt.
- Im Mittelpunkt der Analyse stehen bekannte Sicherheits-Schwachstellen der Dienste und Applikationen auf den Server-Systemen, die von (oder im Auftrag von) österreichischen Unternehmen betrieben werden.
- Basierend auf den Internetdomains der Unternehmen wurden sämtliche Hostnamen dieser Domains ermittelt. Mit der Liste von Hostnamen wurden im nächsten Schritt die IP-Adressen dieser Hostsysteme festgestellt. Die Schwachstellen-Information der einzelnen Hostsysteme stammen aus der Datenbasis der Computer-Suchmaschine Shodan. Die Kritikalität (CVSS) der einzelnen Schwachstellen wurde vom Portal cvedetails.com abgefragt.
- Klassifizierung der Unternehmen nach Anzahl der Assets: Hier werden die Unternehmen aufgrund der Anzahl Ihrer - in der Stichprobe enthaltenen -

öffentlich erreichbaren Server-IP-Adressen bzw. Assets in verschiedene Klassen unterteilt:

  - Sehr klein für 1 IP-Adresse
  - Klein für 2-5 IP-Adressen
  - Mittel für 6-15 IP-Adressen
  - Groß für 15-30 IP-Adressen
  - Sehr groß für mehr als 30 IP-Adressen

- Aufgrund der verwendeten Methode wird davon ausgegangen, dass nicht alle Unternehmen in Österreich in dieser Studie erfasst sind. Außerdem wird davon ausgegangen, dass nicht alle existierenden Systeme der jeweiligen Unternehmen analysiert werden konnten. Tendenziell kann aufgrund der vorgestellten Daten davon ausgegangen werden, dass mit einer höheren Anzahl von Systemen auch die Anzahl der angreifbaren Systeme zunimmt.

  Link auf alle relevanten OSINT2020 Bloginhalte:
  https://www.it-wachdienst.com/tags/osint2020/