Cyber-Angriffe und wie man sein Unternehmen schützt

Vor über 30 Jahren wurde das World Wide Web für die Öffentlichkeit zugänglich gemacht. Seitdem hat es die Welt in vielerlei Hinsicht revolutioniert, es hat die Art und Weise, wie wir kommunizieren, Informationen suchen, einkaufen, arbeiten und lernen komplett verändert.

Text: **Doris Bracher**

NicoElNino / iStock / Getty Images Plus via Getty Images

Gleichzeitig blieb auch die Entwicklung der Kriminalität nicht stehen – sie hat sich ebenso zusehends ins Internet verlagert. In gleichem Maße steigt das Risiko für Unternehmer*innen, Opfer von Internetbetrügern zu werden. Für Landesinnungsmeister KommR Mst. Harald Schinnerl Anlass genug, das Thema „Cyber-Angriffe und wie man sein Unternehmen schützt" für die Mitglieder der Landesinnung der Metalltechniker NÖ aufzugreifen, um über die Machenschaften der Täter zu informieren. Bei der Begrüßung hielt er fest: „Tatsache ist, es gibt nichts, was es nicht gibt. Das Internet scheint der neue ‚Wilde Westen' geworden zu sein."

Zum Fachvortrag begrüßte er Ing. Joseph Riedinger, den ehemaligen Leiter der „Cyber Crime Unit" am Landeskriminalamt NÖ und Inhaber der Technolution Cyber Security Consulting GmbH. Er bestätigte: „Cyberkriminalität ist in jedem Fall eine stark wachsende Bedrohung. Vor Onlinekriminalität kann man sich schützen, besonders Organisationen handeln grob fahrlässig, wenn sie hier keinerlei Vorkehrungen treffen."

Unternehmen sind am häufigsten in Zusammenhang mit Datenmissbrauch involviert, das Spektrum ist breit wie lukrativ. Referent Riedinger: „Cyber Crime ist zu einem immens großen und wirtschaftlich einträglichen Geschäftszeig mutiert. Die Möglichkeit, als Täter*in weitgehend anonym agieren zu können, senkt die Hemmschwelle zur Beteiligung." Dazu ortete er, dass vielen Menschen die Risiken nicht bewusst sind, wenig konkretes Wissen vorhanden ist.

INTERNET – CLEAR WEB & DEEP WEB

Das Internet umfasst das leicht zugängliche Clear Web, wo geshoppt oder gechattet wird, und das Deep Web, zu dem Firmendatenbanken, Server oder Online-Speicher gehören. Dieses stellt mit rund 90 % den umfangreichsten Bereich dar der Zugang ist zudem geschützt. Ein kleiner Teilbereich dieses Deep Web nennt sich Darknet, jener Raum, der auf herkömmliche Weise, wie zum Beispiel durch Suchmaschinen, nicht auffindbar ist, wo die Kommunikation verschlüsselt und die Seiten nicht indexiert werden.

DARKNET – WAS IST ERLAUBT?

Deep Web und Darknet können für nützliche wie schädliche Absichten verwendet werden. Die verschlüsselte Struktur bietet Journalisten oder Verfolgten die Möglichkeit, auf regional gesperrte Inhalte zuzugreifen oder um eine Zensur zu umgehen. Das Darknet ist aber ebenso Handelsplatz für Straftaten und illegale Güter, Kriminelle nutzen die Anonymität ebenso aus. Bezahlt wird meist mit sogenannten Kryptowährungen.

Das Bewegen im Darknet ist entgegen vielen Meinungen auch erlaubt. Es stellt allerdings ein erhöhtes Sicherheitsrisiko dar, da man rasch potenzielles Opfer gewiefter Täter wird. Trotzdem – straffällig wird man erst, sobald illegale Inhalte konsumiert oder heruntergeladen sowie rechtswidrige Waren und Dienstleistungen (Drogen, Waffen etc.) erworben werden.

Doris Bracher

Landesinnungsmeister KommR Mst. Harald Schinnerl, Ing. Joseph Riedinger, Geschäftsführerin Dr. Birgitta Haltmeyer (v.l.n.r.).

FEHLENDE INFORMATION & WENIG WISSEN

Das Fatale ist, dass es für einen kriminellen Akt kein großes Wissen bzw. Vorbereitung braucht. Eine E-Mail unter falschem Namen ist einfach zu schreiben, ein Passwort schnell herausgefunden. Und Auslesegeräte, die das ständig sendende Signal des Autoschlüssels aufnehmen, können unkompliziert erworben werden, womit ein Autodiebstahl in wenigen Minuten erledigt ist. Umso erstaunter ist Experte Riedinger, dass viele Menschen nach wie vor völlig unbedacht agieren. So stellen Handys, die mit dem Auto gekoppelt sind und den Herstellern damit ihre Daten überlassen, gespeicherte Passwörter, freizügig erteilte Befugnisse an Google & Co oder harmlos erscheinende Angaben sicherheitstechnisch eine Gefahr dar, die Kriminellen ihre Arbeit massiv erleichtert.

MASSNAHMEN SCHÜTZEN VOR CYBERANGRIFFE

Wenn Unbefugte versuchen, Computer-Netzwerke oder Systeme zu stören, zu beschädigen oder unerlaubterweise Zugriff zu erhalten, spricht man von einem Cyberangriff. Besonders für Unternehmen können diese zu empfindlichen finanziellen Verlusten aufgrund von Datenlecks, bis hin zu Rufschädigung und rechtlichen Konsequenzen führen. Um solch existenzbedrohende Auswirkungen zu vermeiden, müssen Systeme und Daten geschützt sein. Robuste Sicherheitsmaßnahmen und proaktive Überwachung gewährleisten Sicherheit, dazu sollten regelmäßige Sicherheitsaudits implementiert sein.

Fachleute warnen davor, hier den Sparstift anzusetzen, denn eine Untersuchung und Behebung des Lecks, die Entschädigung betroffener Parteien und ggf. sogar Bußgelder würden Kosten verursachen, die in keinem Verhältnis stehen. Zusätzlich müssen Betriebsunterbrechungen aufgrund von Ausfallzeiten, Produktivitätsverluste und Schäden an Systemen in Kauf genommen werden.

FÖRDERUNG FÜR MITGLIEDER DER LANDESINNUNG DER METALLTECHNIKER NÖ

Betriebe, denen Sicherheit im Umgang mit dem Internet wichtig ist und die jetzt Maßnahmen setzen wollen, erhalten ganz neu für achtstündige Beratungen, bei denen ihre Schwachstellen analysiert werden, Unterstützung. Informationen erhalten Sie bei der Landesinnung der Metalltechniker NÖ. ■

Kontaktdaten und Details zur Förderung finden Sie auf der Homepage unter **https://wko.at/noe/metalltechnik**

KOMMENTAR

ZVG Schinnerl

KommR Mst. Harald Schinnerl, Bundes- und NÖ Landesinnungsmeister Metalltechnik

Parallele Welten

Die digitale Welt bietet Kriminellen ein breites Spektrum an Möglichkeiten, die Deliktformen des Internetbetrugs haben sich auch im Jahr 2023 weiter diversifiziert. Neben einzelnen Tätern dominieren insbesondere organisierte Tätergruppen, die die Anonymität des Internets für ihre Zwecke ausnutzen. Mit minimalen Ressourcen erreichen diese Gruppen eine große Anzahl potenzieller Opfer und erzielen beträchtliche finanzielle Gewinne. Dieser Auszug aus dem jährlichen Report des Bundeskriminalamtes führt ohne Umwege zur Realität. Er weist auch darauf hin, dass Cyberkriminalität den seit Jahren am stärksten wachsenden Bereich in der polizeilichen Anzeigenstatistik darstellt.

Es war eine gute Entscheidung, das Thema für unsere kürzlich abgehaltene Landesinnungstagung aufzugreifen, die Aufmerksamkeit war eindeutiges Indiz. Die Tatsachen sind erschreckend wie alarmierend, Referent Ing. Joseph Riedinger rüttelte mit unzähligen Beispielen aus der Praxis wach.

Für uns Unternehmer*innen heißt es, vorbereitet zu sein. Wenn Sie bisher keine gezielten Maßnahmen gesetzt haben, dann sollten Sie rasch handeln. Cyberangriffe finden auch in diesem Augenblick statt, während Sie diese Zeilen lesen, und sie verursachen häufig einen enormen Schaden. Ein Wegschauen bzw. Ignorieren könnte Sie teuer zu stehen kommen, denn selbstverständlich zahlt man im Ernstfall für den wiederzuerlangenden Zugriff auf die eigenen Daten, die Kriminelle verschlüsselt haben, (fast) jede Summe.

Es gibt ein Bündel an Möglichkeiten, deren Umsetzung Sie höchste Priorität einräumen sollten. Vergessen Sie nicht darauf, Ihre Mitarbeiter zu sensibilisieren, sie zu schulen und ihnen aktuelle Informationen zukommen zu lassen. Auch Sie sollten sich ob des Risikos bewusst sein, Ihr Verhalten gegebenenfalls ändern. Wissen schützt und stärkt das Bewusstsein, wodurch unbedachte Handlungen vermieden werden können.

Ich lege Ihnen ans Herz, die Gesamtstrategie einem Experten zu überlassen. Nutzen Sie dazu unsere neue Förderung, lassen Sie sich beraten.

Zum Jahresende bedanke ich mich für die gute Zusammenarbeit. Ich wünsche Ihnen Zufriedenheit, Dankbarkeit, Gesundheit und schöne Feiertage.

Ihr Innungsmeister KommR Mst. Harald Schinnerl