23.06.2022 – 10:30 Uhr

Swissmem Medienmitteilung: Illegale Angriffe: 70 Prozent der Swissmem Mitgliedfirmen betroffen

Zürich (ots) -

Illegale Angriffe: 70 Prozent der Swissmem Mitgliedfirmen betroffen

Im Zeitalter der Digitalisierung bieten Industriebetriebe für Cyberkriminelle besonders grosse Angriffsflächen. Cyberattacken, aber auch physische Angriffe, sind heute eine konstante Bedrohung. Es kann jedes Unternehmen unabhängig seiner Grösse treffen. Das Schadenspotenzial ist enorm und kann im Extremfall die Existenz einer Firma gefährden. Eine Umfrage unter den Swissmem Mitgliedfirmen zeigt, dass in den letzten zwei Jahren 70 Prozent der antwortenden Unternehmen Ziel von mindestens einer Attacke wurde. Entsprechend ist die Sensibilisierung zu diesen Risiken in den Firmen hoch. In fast allen Betrieben werden gezielt Präventionsmassnahmen umgesetzt. Sie haben dazu geführt, dass 82 Prozent der als sehr schwerwiegend eingestuften Angriffe keine Folgen hatten oder diese kurzfristig behebbar waren. Die Aufmerksamkeit darf jedoch nicht nachlassen.

Swissmem hat in Zusammenarbeit mit dem Institut für Strafrecht und Kriminologie der Universität Bern eine Umfrage unter 1200 Swissmem-Mitgliedfirmen zu Fragen der Sicherheit durchgeführt. 271 Firmen haben den Fragebogen ausgefüllt. Aus den Antworten geht hervor, dass in den letzten zwei Jahren 70 Prozent der befragten Unternehmen Ziel von mindestens einer Attacke wurde. Einzelne Firmen wurden mehr als 20-mal angegriffen.

Mit 50 Prozent war CEO-Fraud die häufigste Angriffsart. Dabei versuchen Kriminelle unter Verwendung einer falschen Identität Geldüberweisungen zu erwirken. Von Phishing-Attacken berichten 43 Prozent der Befragten. Ziel dieser Angriffe ist es, Zugang zu den ICT Systemen zu erhalten, um illegal an wertvolle Daten zu gelangen. Jedes fünfte Swissmem Mitglied (20,7%) wurde Opfer von Schadsoftware wie Viren, Würmern und Trojanern sowie von Hackerangriffen. Social Engineering betraf jedes sechste Unternehmen (16,2%). Hier werden Mitarbeitende gezielt ausspioniert, um an vertrauliche Informationen zu gelangen. Die Mehrheit der angegriffenen Firmen (58,3%) glaubt, dass sie zufällig als eines von vielen Unternehmen tangiert wurde. Über ein Fünftel der betroffenen Firmen (21,4%) geht hingegen davon aus, dass sie gezielt angegriffen wurden.

Den beiden Studienleitenden der Universität Bern, Prof. Ueli Hostettler und Dr. Anna Isenhardt, fiel folgendes auf: "Die antwortenden Unternehmen sind insbesondere von Angriffen aus dem Bereich Cybercrime betroffen. Das ist ein Deliktsbereich, in dem in den letzten Jahren im Vergleich zu anderen Straftaten international ein Anstieg zu verzeichnen war. Sehr viele der seit Bestehen des Unternehmens berichteten Cybercrime-Angriffe scheinen erst in den letzten zwei Jahren erfolgt zu sein."

Swissmem Mitgliederfirmen wissen, dass illegale Angriffe schwerwiegende Folgen haben können. Das gilt für Grossfirmen und KMU. Im Durchschnitt haben sie 25 Schutz- und Interventionsmassnahmen im Einsatz. Diese Massnahmen haben dazu geführt, dass 82 Prozent der Vorfälle keine Folgen (13,7%) hatten oder die Angriffe kurzfristig behebbar waren (68,4%). Dennoch: Bei jedem sechsten Unternehmen (15,8%) führte der Angriff zu spürbaren betrieblichen Einschränkungen. Vor allem Attacken aus dem Bereich Cybercrime können schwerwiegende und kostspielige Folgen haben. In fast einem Fünftel (18,2%) der antwortenden Unternehmen verursachten die Angriffe einen Schaden zwischen 100'000 und einer Million Franken. Je nach Unternehmen kann das existenzbedrohend sein.

Martin Hirzel, Präsident Swissmem, sagt zu den Umfrageergebnissen: "Ich bin froh, dass innerhalb der Swissmem Mitgliedschaft eine hohe Sensibilisierung zu Cyberangriffen und physischen Bedrohungen besteht. Die Aufmerksamkeit darf jedoch nicht nachlassen. Jeder Betrieb muss technologisch und organisatorisch stets vorbereitet sein, um solche Attacken abwehren zu können. Dies sicherzustellen ist Chefsache".

Digitalisierung versus Cyber-Sicherheit

Viele Industrieunternehmen sehen sich angesichts dieser Bedrohungslage in einem Zielkonflikt. Einerseits sind sie gefordert, in die Digitalisierung der betrieblichen Prozesse, Produkte und Dienstleistungen zu investieren. Das erfordert eine teils unternehmensübergreifende und immer intensivere Vernetzung der Systeme. Andererseits erfordert der Schutz eben dieser Systeme, bei der Vernetzung vorsichtig vorzugehen und geeignete Abschirmungsmassnahmen zu treffen.

Bei der Auflösung dieses Zielkonfliktes kann die Initiative "Industrie 2025" helfen. Sie wird von den Verbänden Swissmem, asut und SwissTnet getragen. Sie hat sich zum Ziel gesetzt, die digitale Transformation auf dem Werkplatz Schweiz voranzutreiben. Unter der Bezeichnung "Security 2025" wurde ein spezielles Angebot für Industriebetriebe geschaffen. Dabei helfen Experten insbesondere KMU, die Sicherheitsthemen anwendungs- und praxisbezogen anzugehen. Die Bedürfnisse der vernetzten Industrie werden dabei speziell berücksichtigt.

Pressekontakt:

Weitere Auskünfte erteilen:

Jonas Lang, Stv. Leiter Kommunikation
Telefon +41 44 384 48 33 / Mobil +41 79 777 41 36
E-Mail: j.lang@swissmem.ch

Philippe Cordonier, Responsable Suisse romande
Tel. +41 21 613 35 85 / Mobile +41 79 644 46 77
E-Mail p.cordonier@swissmem.ch