CYBERSECURITY – Trojaner, Malware, Phishing, Ransomware. Aufgrund der aktuellen Brisanz und einer Häufung erfolgreich durchgeführter Angriffe, nimmt unser Cybersecurity-Experte, Chris Eckert, eine zweiteilige Auslegeordnung für KMU vor. Er zeigt am Beispiel der Ransomware auf, wie die Attacken erfolgen, Schäden entstehen und wie man sich wehrt.

Die Angriffe nehmen bedrohlich zu

Wo liegt die Gemeinsamkeit einer mittelgrossen Schreinerei, eines Start-ups in der Modebranche, einer Forschungsanstalt, eines nachhaltigen Lebensmittelproduzenten sowie eines Regionalspitals? Alle sind heute von Kompromittierungen ihrer vertraulichen Daten und Informationen bedroht.

In regelmässigen Abständen warnen Sicherheitsexperten sowie IT-Security-Anbieter vor neuen Angriffsmethoden im gesamten Bereich der Informationstechnologie. Mehr Varianten und neuartige Vorgehensweisen tauchen auf, dabei sind auch ältere Angriffsvarianten immer noch erfolgreich …

Wie die Häufung – im zunehmenden Masse auch in der Schweiz medial publiziert – der vergangenen Monate zeigt, tun sich Firmen und Institutionen in der Schweiz offenbar immer noch schwer, geeignete und einfache Schutzmassnahmen zu prüfen und einzurichten. Während der Sommerferien wurden Ransomware-Attacken auf eine Klinikgruppe, verschiedene Traditionsfirmen und Industrieunternehmen, eine Universität in Liechtenstein sowie eine grössere Gemeindeverwaltung in der Westschweiz bekannt. Auch eine internationale Beratungsfirma war nicht gefeit. Viele Angriffe auf kleinere KMU in der Schweiz erfolgten zur selben Zeit, kamen aber nicht an die Öffentlichkeit.

Leider wird in den meisten Fällen gewartet, bis es zu spät ist. Zwei hauptsächliche Glaubensthesen herrschen immer noch bei vielen Verantwortlichen – egal ob Chef, Inhaber oder Verwaltungsrat – vor. In jedem Schadensfall ist die Meinung irrig, zugleich trügerisch und ebenfalls brandgefährlich. Es heisst dann entweder «bei uns kann das nicht passieren, denn wir sind für Hacker nicht interessant» oder aber «Wir schauen dann schon, wenn wir angegriffen worden sind» …

Blockiert: Die Angreifer fordern Lösegeld, um die verschlüsselten Daten und Informationen wieder freizugeben.

Bild: 123RF

Wie funktioniert denn nun ein Ransomware-Angriff?

Es handelt sich um eine Schadsoftware, welche ein Computersystem in einer Firma, Institution oder Organisation infiziert, um die Verantwortlichen zu erpressen. In den meisten Fällen wird (Löse-)Geld gefordert. Die Daten der Betroffenen werden vollständig verschlüsselt, eine Aufrechterhaltung der Produktion oder des Onlineshops beispielsweise ist kaum mehr möglich. Wird Lösegeld für kritische Daten erpresst, wird Ihr Unternehmen mit teilweise grösstmöglichem Schaden effektiv lahmgelegt. Lieferanten können nicht mehr liefern, Kunden nichts mehr bestellen und die Mitarbeitenden können ihre Arbeitsprozesse nicht mehr ausführen. Dazu kommt das Kommunikationschaos, intern wie extern, und ein Reputationsschaden in nicht bezifferbarem Ausmass. Das ist nicht einfach nur ärgerlich. Es kann auch existenzbedrohend werden.

Wird das geforderte Lösegeld bezahlt, erhält der Geschädigte ein Tool, um die verschlüsselten Daten wieder brauchbar zu machen. Als perfide Steigerung des kriminellen Vorgehens hat sich in letzter Zeit die sogenannte doppelte Erpressung entpuppt: Die Angreifer drohen mit der Veröffentlichung von vertraulichen oder geheimen Geschäftsdaten/Informationen über Personen, beispielsweise Patientendaten, Zugangscodes für Systeme oder Passwörter. Als wäre die Verschlüsselung sowie der Stillstand des Betriebes schon nicht schlimm genug, wird so zusätzlich Druck auf die Opfer ausgeübt.

Aufgrund des rasanten Aufschwungs des meist erfolgreichen Einsatzes von Ransomware in den letzten beiden Jahren, stellt das lukrative Milliardengeschäft für die Cyberkriminellen ein lohnendes Geschäftsmodell dar. Immer mehr kriminelle Gruppierungen – meist aus dem fernen Ausland – sind auf die Angriffswelle aufgesprungen, denn es bestehen kaum Risiken und das Geschäft kann vielfältig skaliert werden. In den Entwicklungs- und Schwellenländern sind sie vor einer Verfolgung sicher und werden oft von den lokalen Behörden in Ruhe gelassen. Die mangelnde Kooperation, kaum umsetzbare Gesetze und die fehlenden Ressourcen samt ungenügendem Know-how der Strafverfolgungsbehörden auf internationaler Ebene sind untaugliche Werkzeuge gegen diese Form von Kriminalität.

Was ist das Ziel solcher Angriffe?

Besonders lohnende Ziele sind Firmen, Institutionen und Private, welche auf funktionierende Informatiksysteme oder vernetzte Elektronik zwingend angewiesen sind und bei einem Ausfall ein existenzieller Schaden verursacht wird: KMU und Grosskonzerne im Industrie-, Forschungs-, Kommunikations- und Dienstleistungssektor; ebenso wie Spitäler, Anwalts- und Treuhandkanzleien, Vermögensverwalter, Blaulichtorganisationen und Behörden.

Das oberste Ziel ist immer das Gleiche: möglichst viel Lösegeld zu erpressen. Die Angreifer überprüfen im Internet oder mittels Informationsbeschaffung, ob Ihr Unternehmen erfolgreich wirtschaftet oder gar an der Börse ist. Wenn ja, fordern die Kriminellen eine angemessene Summe an Lösegeld. Der Zustand der Informationssicherheit einer Organisation ist ebenfalls entscheidend. Wer schlecht gegen Risiken und Angriffsszenarien geschützt ist, kann leichter geschädigt werden: Phishing-E-Mails, Social-Engineering-Aktivitäten, mangelhafte Prozesse, nicht sensibilisiertes Personal, lückenhafte physische Sicherheit sowie technische und elektronische Schlupflöcher einer Organisation, schlichtweg Mängel beim Daten- und Informationsschutz, dienen geradezu als willkommene und einfache Einfallstore für Vorbereitungshandlungen der Hacker.

Im 2. Teil zu diesem Thema *(sgz vom 1. Oktober 2021)* wird auf das Ausmass der Schäden sowie umsetzbare Massnahmen gegen Ransomware-Angriffe eingegangen. Vorneweg fünf Tipps in Kurzform für einen besseren Schutz:

- Sicherungskopie/Backup Ihrer Daten (möglichst offline und extern gelagert)
- Software aktuell halten
- Kritischer und vorsichtiger Umgang mit E-Mails
- Virenschutz und Firewall aktualisieren
- Verdächtige E-Mail-Anhänge blockieren, keinesfalls öffnen!

Chris Eckert

Mehr Auskünfte und gezielte Schulungen erteilt Ihnen: **www.swissbp.ch**

DER AUTOR

Chris Eckert ist Founding Partner der Swiss Business Protection AG. Er verfügt über mehr als 30 Jahre kriminalistische Erfahrung, erworben bei der Kantonspolizei Zürich sowie der Bundeskriminalpolizei.
www.swissbp.ch

UNTERNEHMENSSCHUTZ

Neuer Lehrgang

Zugeschnitten auf den umfassenden Unternehmensschutz für KMU in der Schweiz wurde ein neuer Lehrgang erschaffen. Der CAS «Business Protection» an der Hochschule für Wirtschaft HWZ in Zürich startet am 18. Februar 2022 und dauert berufsbegleitend 18 Tage. Es sind noch Studienplätze frei: