CYBERATTACKEN – Aufgrund der aktuellen Brisanz sowie vieler erfolgreich durchgeführter Cyberangriffe wird in einer dreiteiligen Serie diese Thematik für unsere KMU hervorgehoben. Am Beispiel der aktuell vorherrschenden Methode, dem sogenannten Ransomeware-Angriff, zeigen wir auf, wie solche Attacken erfolgen, welche Schäden entstehen – und womit man sich erfolgreich wehren kann.

Immense Schäden durch Angriffe

In der Gewerbezeitung vom 17. September wurde der Fokus auf das Funktionieren eines Ransomware-Angriffs sowie das erklärte Ziel der kriminellen Hacker gelegt. Im heutigen zweiten Teil dieser Thematik wollen wir etwas Licht in das Ausmass der Schäden bringen.

Verheerende Schäden auf Unternehmen und Mitarbeitende

Bis vor wenigen Jahren genügten nach einem klassischen Einbruchsdiebstahl in ein Firmengebäude eine Anzeigeerstattung bei der Polizei, das Reparieren des zerstörten Fensters durch den Schreiner, die Schadenmeldung an die Versicherung und bestenfalls das Anbringen von einbruchsicheren Fenstern. Damit war der Fall erledigt – aus den Augen aus den Sinnen. Sichtbarer Angriff, eingrenzbarer Schaden, Problem gelöst.

Heute bewegen wir uns auf einer völlig anderen, unsichtbaren Ebene: Kaum bezifferbarer Schaden, in den meisten Fällen ein Lahmlegen der Produktion für lange Zeit, meist kaum Reaktionszeit für interne sowie externe Kommunikation, fehlendes Know-how für die Ereignisbewältigung, ungewisser Fortgang der Geschäftstätigkeit und ein möglicher Reputationsverlust bis hin zur Schliessung des Unternehmens. Von den blank liegenden Nerven, schlaflosen Nächten und den immensen Gesamtkosten – inkl. Erpressungssumme – ganz zu schweigen.

Wie schon erwähnt, kann heutzutage jede Firma, ob klein, mittel, oder gross, egal auch welche Branche, Opfer eines Ransomware-Angriffs werden. Institutionen und Private nicht ausgeschlossen! Die Frage ist leider nicht mehr ob, sondern wann man von einem Angriff heimgesucht werden wird. Überall dort, wo viel Lösegeld zu erpressen sein könnte, ist es für die Täter interessant. Ein besonderes Interesse erwirken Firmen, die bekanntermassen erfolgreich wirtschaften, existenziell auf eine reibungslos funktionierende Informatik angewiesen sind sowie ungenügende Sicherheit in den Bereichen Informations- und Datenschutz aufweisen *(vgl. auch sgz vom 17. September)*. Cyberattacken sind kaum vorhersehbar im Vergleich zu vielen anderen Unternehmensrisiken, niemand ist davor natürlich gefeit. Man muss aktiv etwas dagegen tun und sich damit befassen. Sicherheit und Unternehmensschutz sind Chefsache! Wegducken, warten, beten und hoffen ist definitiv der schlechteste Ratgeber!

Die Realität überholt uns …

Neuste Studien *(Quelle: 2021 GDPI Dell Technologies)* zeigen auf, dass heute die Firmen mit rund zehn Mal so grossen Datenmengen operieren als noch vor fünf Jahren. Tendenz massiv steigend – je mehr Daten und Informationen, desto anfälliger und grösser der Angriffsvektor. Über drei Viertel der befragten Firmenverantwortlichen sind der Meinung, dass sie mit ihren bisher vorhandenen Produkten und Lösungen alleine im Bereich der Datensicherung wohl nicht bestens gerüstet sind. Mehr als 60 Prozent scheinen der Auffassung zu sein, dass ihre Datensicherungsmassnahmen bei einem konkreten Ransomware-Angriff vermutlich nicht genügen werden. Fast zwei Drittel wagen zu behaupten, dass sie nach einer Ransomware-Attacke wohl nur noch wenig wichtige Geschäftsdaten wiederherstellen können. Als Unternehmer versetzen mich solche Zahlen in ungläubiges Staunen. Gleich gelagerte Aussagen von Geschäftsführern und Unternehmensinhabern erschrecken mich zutiefst. Ich frage mich schon lange, ob seitens der Firmenverantwortlichen wirklich weitergedacht oder ob die Situation einfach hingenommen wird? Sind sie sich ihrer Verantwortung gegenüber Ihres Unternehmens sowie all ihrer Mitarbeitenden wirklich nachhaltig bewusst?

Wie äussern sich die Schäden?

Allgemein zeichnet sich betreffend Daten und Informationen eine rasante Steigerung der Sicherheitsrisiken für Private, Institutionen und Unternehmen ab. Ging man im Sommer 2019 noch von einem täglich geschätzten Wert von durchschnittlich 240 000 Cyberangriffen weltweit aus, waren es im Sommer 2020 bereits über 3,4 Millionen Cyberattacken täglich. Die Zahlen fürs 2021 liegen noch nicht vor, dürften aber nochmals einen Sprung nach oben gemacht haben.

Vorhandene Zahlen aus den Industrieländern zeigen auf, dass die durchschnittliche Lösegeldforderung von den Erpressern bei den KMU im Schnitt rund 6000 Franken beträgt, Tendenz steigend. Die Gesamtkosten für Sofortmassnahmen, Systemausfälle, Aufarbeitungs- und Beratungsdienstleistungen sowie Instandstellungs- und Rettungsarbeiten sind sehr viel höher. Im Schnitt wird das 40- bis 50-Fache des Lösegelds geschätzt. Reputationsschäden, die Monate bis Jahre anhalten können, sind noch nicht eingerechnet. Zunehmend erfolgt auch eine zweite Erpressungswelle: Wenn in grosser Not seitens der Geschädigten das Lösegeld bezahlt wird, erscheint eventuell eine Nachforderung, ehe dann die Daten wieder entschlüsselt zur Verfügung gestellt werden. Zur Steigerung der negativen Einwirkung setzen die Erpresser auch noch die doppelte Erpressung ein, d. h. sie drohen mit der Veröffentlichung ihrer vertraulichen und geheimen Firmeninformationen. Bestehen also keinerlei gesicherte Daten oder aktuelle Back-ups ausserhalb des Netzwerks, ist man als geschädigte Organisation auf Gedeih und Verderb am Gängelband der Kriminellen.

Wo ist anzusetzen?

Der Umstand lässt sich auch nicht durch eine Versicherungspolice einfach beheben, weil diese erst zum Tragen kommt, wenn Sie schon erfolgreich angegriffen worden sind. Der alleinige Abschluss einer sogenannten Cyberversicherung mit (noch) günstigen Prämien genügt bei Weitem nicht und ist als einzige, losgelöste Massnahme in etwa mit der Einnahme eines tief dosierten Schmerzmittels bei einer Hirnhautentzündung zu vergleichen. Symptombekämpfung wirkt vielleicht ein paar Tage zur mentalen Beruhigung, die Delegation des Gesamtthemas Sicherheit und Resilienz an eine untergeordnete Stelle innerhalb des Betriebs löst das strategische Problem nur oberflächlich. Risiken im Bereich der Cyberangriffe oder -kriminalität, besser noch bei der allumfassenden Unternehmenssicherheit, sollten bei allen Firmen und Institutionen auf die oberste Führungsstufe angehoben und ständig bewirtschaftet werden. Nirgends im Leben gibt es eine 100-prozentige Sicherheit; ebenfalls ist es illusorisch, Cyber-Risiken komplett beseitigen zu können. Aber man kann eine Menge tun, um die Eintrittswahrscheinlichkeit zu reduzieren sowie die Reaktionszeit bei der Aufarbeitung und Behebung des Schadenfalls zu verringern!

Proaktive Massnahmen bei der Prävention und Sensibilisierung aller Mitarbeitenden sind der erste und wichtigste Schritt für die Steigerung Ihrer integralen Sicherheit. Folgende Hauptthemen sind zu berücksichtigen und werden im dritten und letzten Teil *(sgz vom 22. Oktober)* eingehend behandelt:

- Informationssicherheit
- Physische Sicherheit
- Schwachstelle Mensch
- Notfallplan, Awareness

Chris Eckert

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