Unternehmen gehackt
Wer haftet dafür?

isential gmbh
IT Solution Provider

18. April 2017

EINLEITUNG

Augen verschließen und Problem vertagen – es riecht nicht, man hört es nicht und man kann es auch nicht sehen. Wenn man es jedoch spürt, ist es zu spät und man hat den Kampf bereits verloren.

Die Zahlen sind erschreckend und man kann nur mutmaßen, wie hoch diese wirklich sind, denn viele Unternehmen melden Hackerangriffe aus unterschiedlichen Gründen nicht und werden somit statistisch nicht erfasst: Im Jahr 2016 wurde in Deutschland ein Fünftel der mittelständischen Unternehmen gehackt.

DON QUIJOTE UND DER KAMPF GEGEN WINDMÜHLEN

Es ist in der Tat wie der berühmte Kampf gegen Windmühlen: Kriminellen Hackern gelingt es immer wieder, sich in fremde IT-Systeme von Unternehmen einzuhacken – Tendenz stark steigend. Man könnte davon ausgehen, dass angesichts der alarmierenden Zahl von Angriffen Unternehmen in ständiger Alarmbereitschaft stehen und alles Mögliche daransetzen, wiederholte Hackerangriffe abzuwehren. Ist es auch so?

Die beunruhigende Realität

Die Realität sieht komplett anders aus: Gerade, wenn es um die Sicherheit der IT-Systemen im eigenen Unternehmen geht, werden die notwendigen Sicherheitsmaßnahmen häufig vernachlässigt. Fehlende, falsche oder veraltete Sicherheitssoftware sind Beispiele für lückenhafte IT-Systeme. Aber auch die Netzwerkverwaltung ist in vielen Fällen unzureichend und führt insbesondere in kleineren Unternehmen zum Teil zu gefährlichen Fehlkonfigurationen – hier fehlt oft das Know-how, um Netzwerke professionell zu planen und abzusichern. Die Sensibilisierung von Mitarbeitern durch Schulung und Auferlegung klarer Regeln ist ebenfalls in den meisten kleineren Unternehmen unzureichend bzw. meistens erst gar nicht vorhanden.

Aber auch Unternehmen, die in Sicherheit investieren, laufen oft in die gleiche Falle: Hacker finden immer wieder neue Mittel und Wege, in fremde Systeme einzudringen. Deswegen müssen die Sicherheitsmaßnahmen im Unternehmen stets angepasst bzw. erweitert werden, um mit dieser beunruhigenden Entwicklung Schritt halten zu können. Investiert das Unternehmen nicht laufend in Sicherheit, veralten seine Sicherheitssysteme und -konzepte sehr schnell und werden selbst zu einem Risikofaktor.

Wer trägt die Verantwortung bei einem Hackerangriff?

Leider ist die rechtliche Lage zurzeit nicht eindeutig und so gibt es keine klaren Regeln. Unternehmen werden selten zur Verantwortung gezogen und so leiden am Ende andere, deren Daten als Zielscheibe für Hacker fungieren. Daher ist die Forderung nach Sicherheitsstandards mehr als gerechtfertigt.

Um allerdings ein Unternehmen zur Rechenschaft ziehen zu können, muss ihm Fahrlässigkeit nachgewiesen werden. Als Beispiel dazu zählen die fehlende oder mangelnde Aktualisierung von Abwehr-Systemen oder wenn das Unternehmen Sicherheitslücken einfach ignoriert.

Auch sehr wichtig: Verfügt das Unternehmen über eine Person, die ausschließlich für die IT-Sicherheit verantwortlich ist? Firmen mit derartigen Personen sind nämlich weitaus mehr um lückenlose Sicherheit bemüht und haben auch nachweislich weniger Schäden durch Angriffe auf die Systeme zu bewältigen.

Laut Umfragen fordert eine große Mehrheit der befragten Unternehmen (neun von zehn Vorstandsvorsitzenden), dass Unternehmen, die sich nicht ernsthaft um ihre Datensicherheit bemühen, in Haftung genommen werden sollten. Klare Regeln und standardisierte Vorschriften werden also auch in den Führungsetagen der Unternehmen begrüßt.

Das IT-Sicherheitsgesetz des BSI (https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/IT-SiG/it_sig_node.html) versucht, deutliche Standards vorzugeben. Allerdings sind diese leider unklar definiert. Ein großes Problem ist die weitläufige Interpretierbarkeit der verwendeten Begriffe. Diese Begriffe sorgen für ein lückenhaftes Verständnis. So werden moderne Technologien als „angemessene Vorkehrungen“ bezeichnet oder Straßen mit Internetdienstleistern verglichen, um sie unter dem Begriff „kritische Infrastrukturen“ gleichzusetzen – das ist alles andere als eindeutig.

Durch die unklaren Definitionen des IT-Sicherheitsgesetzes kann die Frage der Haftung im Falle eines Hackerangriffs und des sich daraus ergebenden Datenmissbrauchs nicht immer eindeutig definiert werden. Daher gehen viele Unternehmen dazu über, diese Punkte mit ihren Geschäftspartnern bereits im Vorfeld eindeutig zu definieren und vertraglich festzuhalten: Möchte z. B. ein Unternehmen als Zulieferer eine Geschäftsbeziehung mit einem anderen Unternehmen eingehen, werden bezüglich IT-Sicherheit klare Vereinbarungen getroffen, die in aller Regel durch Audits in periodischen Abständen kontrolliert und eventuell angepasst werden. Aber wie sieht es bei einem Hackerangriff aus, wenn solche Vereinbarungen fehlen?

Anreiz durch Versicherung

Wie bereits im vorigen Abschnitt erläutert, bietet die geltende Rechtslage nicht genügend Anlass, Sicherheitsvorkehrungen vorbildlich einzuhalten. Nun muss anders dafür gesorgt werden: zum Beispiel in Form von sog. Cyber-Versicherungen. Diese können dazu führen, den IT-Sicherheitsansatz eines Unternehmens grundlegend zu verändern. Nach Angaben von Analysten soll sich das Volumen des Versicherungsmarkts in den nächsten fünf Jahren auf ca. 7 Milliarden Euro verdreifachen. Dass ein Unternehmen, welches sich finanziell gegen einen Hackerangriff absichert, weniger risikofreudig mit dem Thema Datensicherheit umgeht, dürfte als unmittelbare Folge angesehen werden.

Verantwortung übernehmen

Unternehmen sind für eine umfassende IT-Sicherheitsstrategie selbst verantwortlich. Solange der Gesetzgeber keine rechtlich klar definierten Regeln schafft, werden sich viele Unternehmen nicht um die Einhaltung grundlegender Sicherheitsmaßnahmen bemühen. Abhilfe könnten hier z. B. Cyber-Versicherungen leisten, die für transparenten Sicherheitsstandards sorgen könnten.

Es sollte jedoch jedem Unternehmer klar sein, dass die Vernachlässigung von IT-Sicherheitsstandards nicht nur kurzsichtig ist, sondern sie kann sogar das Ende eines Unternehmens bedeuten. Gerade in einem hochentwickelten Land wie Deutschland, dessen größte Ressource das Know-how ist, kann das unkontrollierte Abfließen von Wissen den Ruin eines Unternehmens bedeuten, das ganz abgesehen vom Imageverlust bei Kunden und Lieferanten.

Die Frage der Haftung ist unter diesen Gesichtspunkten fast zweitrangig: Jedes Unternehmen hat eine Verantwortung gegenüber seinen Mitarbeitern und Geschäftspartnern. Die Vernachlässigung der IT-Sicherheit wird in erster Linie immer das gehackte Unternehmen schwer treffen.

Ein abgewehrter Hackerangriff ist sicher schwer finanziell zu quantifizieren. Dennoch möchte niemand das am eigenen Leibe erfahren, nur um einen Vergleich ziehen zu können, ob die finanziellen Folgen eines Angriffes teurer oder preisgünstiger als die Abwehr sind. Der nächste Angreifer steht schon vor der Tür.

Sorgen Sie daher für ein ausgereiftes und zukunftssicheres Sicherheitskonzept. Wir helfen Ihnen gerne dabei.