Cybersecurity-Budgetierung

Eine grosse Herausforderung für KMU.

Ausgabe
September 2019

Autor Levente J. Dobszay

Bezugsquelle Electrosuisse | Luppmenstrasse 1 | Postfach 269 | 8320 Fehraltorf
electrosuisse.ch/cybersecurity

Cybersecurity-Budgetierung: eine grosse Herausforderung für KMU

Sicherheit hat ihren Preis und ganz besonders Cybersecurity. KMU, die der Cybersicherheit bis anhin wenig Aufmerksamkeit geschenkt haben und bescheidene Budgets dafür einsetzen, sind gefordert, ihre Mittel zugunsten merklich höherer Investitionen in die Cybersicherheit sinnvoll aufzustocken.

Diskrepanz zwischen Risiken und Sicherheitsbudgets

Die Bedrohungslandschaft erweitert sich laufend, während die Cybersecurity-Budgets gerade bei KMU mehrheitlich immer noch stagnieren. Die digitale Sicherheit eines Unternehmens kann jedoch nur mit einem sinnvollen Budget gewährleistet werden. Verschiedene Studien zeigen allerdings, dass die Investitionen in die Cybersicherheit nicht mit jenen der Digitalisierung mithalten können. Die Absicht, mehr in eine zeitgemässe Cybersecurity zu investieren, liegt zwar im Trend, mehr als drei Viertel der Unternehmen verfügen aber nicht über ein ausreichendes Budget, um das nötige Mass an Cybersicherheit und Widerstandsfähigkeit zu gewährleisten. Cybersecurity ist bei der Mehrheit der Unternehmen kein integraler Bestandteil der Unternehmensstrategie und der operativen Pläne. In Anbetracht, dass über 90 Prozent der Unternehmen dem Thema angeblich einen hohen Stellenwert beimessen, erstaunt dies sehr.

Während ein Abfluss von schützenswerten Daten mit persönlichen Konsequenzen für Kunden, Führungskräfte und Mitarbeiter, einem damit einhergehenden Vertrauensverlust und allfälligen Bussgeldern für verschiedene Betriebe noch verkraftbar sein dürften, kann ein längerer Betriebsunterbruch oder der Totalverlust geschäftskritischer Daten nicht nur zu Reputationsschäden oder Haftungsansprüchen sondern zu existenziellen Liquiditätsproblemen durch Produktivitäts- und Umsatzverluste sowie ungeplante Wiederherstellungskosten führen oder sogar das plötzliche Aus bedeuten. Diese Risiken werden von der grossen Mehrheit der Unternehmen immer noch massiv unterschätzt.

Auch wenn sich die Ausgaben für die digitale Sicherheit in Unternehmen in den letzten 10 Jahren im Durchschnitt etwa verdoppelt haben, können sie noch lange nicht mit der ungleich stärker gewachsenen Bedrohungslage mithalten. Permanente Cyber-Attacken sind die Normalität, wobei sich die Angriffsvektoren ständig verschieben und die Schadsoftware immer ausgefeilter und multifunktionaler wird. Die Angriffe und Vorfälle nehmen dabei in Frequenz und Heftigkeit stark zu. Cyber-Kriminelle geben zudem global zehnmal mehr Geld für Tools und Informationen aus als Unternehmen für ihre Sicherheit. Dieser wachsenden Bedrohungslage stehen allgemein sehr bescheidene Cybersecurity-Budgets gegenüber, die nur selten risikogerecht und oft falsch alloziert sind. Trotzdem haben viele Unternehmen Angst, zu viel und unnötig in ihre Cybersicherheit zu investieren.

Die Schadenssumme eines Cyber-Vorfalls einschliesslich aller Folgekosten kann auch bei einem KMU in die Millionen gehen. Bereits der Einsatz von hinzugezogenen Sicherheitsexperten bei einem Schadsoftwarebefall kostet schnell mehr als 50’000 Franken. Innerhalb eines Jahres wird aktuell jedes zwanzigste Schweizer KMU zum Opfer von Ransomware (Erpressungs-Trojaner) und mehr als ein Drittel wird von Malware

wie Viren oder Trojanern befallen. Trotzdem beurteilen gut die Hälfte den eigenen Schutz als gut bis sehr gut und nur die wenigsten erachten die Risiken von Cyber-Vorfällen als existenzgefährdend. Realistisch gesehen können aktuell jedoch weniger als 10 Prozent der Unternehmen als genügend gegen Cyber-Risiken gewappnet bezeichnet werden. Dazu gehören vor allem Firmen, deren Existenz schon länger von ihrer Cybersicherheit abhängt und die sich entsprechend nicht erst seit gestern darum kümmern. Andere haben einen Cyber-Vorfall schon gar nicht überlebt.

Gemäss Schätzungen überleben nur 40 Prozent der Unternehmen, die einen schweren Vorfall erlitten haben, die darauffolgenden zwei Jahre. Oftmals wird Cybersecurity auch deshalb zu tief budgetiert, weil ein markant höheres Budget im Vergleich zum Vorjahr Fragen nach sich zieht und die Verantwortlichen eine Blossstellung und Schuldzuweisungen für bisherige Versäumnisse fürchten. Oftmals werden daher veraltete Sicherheitslösungen, die sogar ihr supporttechnisches Lebensende schon überschritten haben, nicht durch neue Sicherheitslösungen auf dem Stand der Technik erneuert. Dies kann fatale Folgen haben.

Cybersecurity-Kosten richtig budgetieren

Als Cybersecurity-Kosten werden allgemein jene Kosten bezeichnet, welche für Schutz-, Detektions- und Behebungsmassnahmen gegen externe oder interne Angriffe verursacht werden und über die bedrohungsfreien Betriebskosten hinausgehen, obwohl Cybersecurity auch die Risiken durch digitale Elementarschäden beinhaltet.

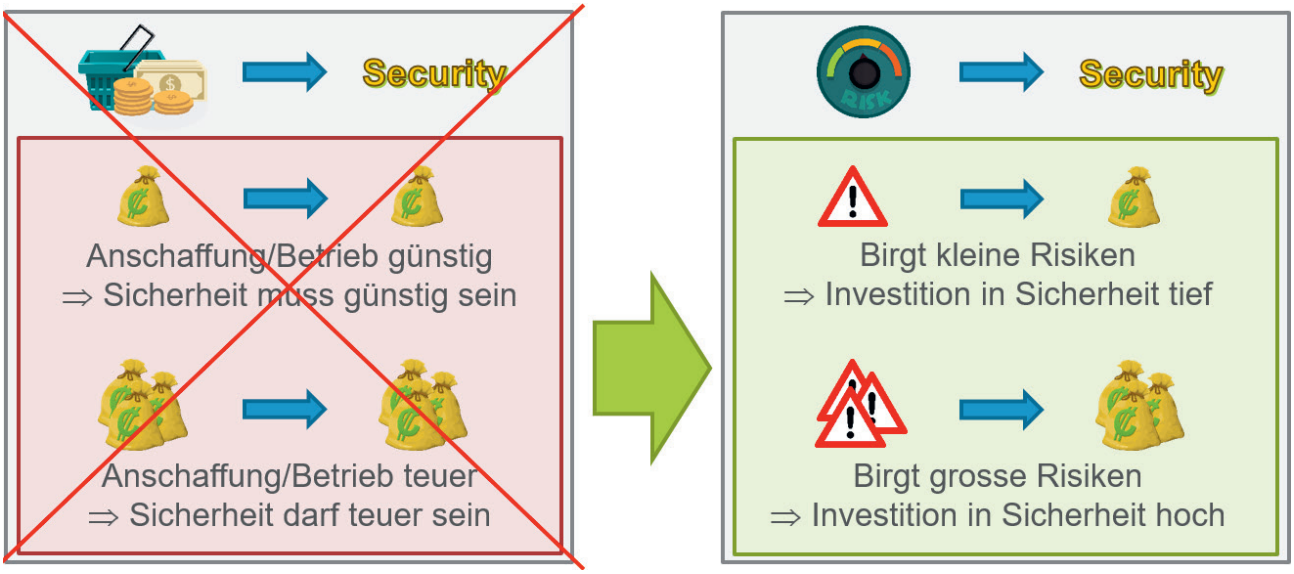

Abbildung 1: Risikobasierte Investition in Cybersecurity

Viele Unternehmen budgetieren die Cybersecurity-Kosten in Abhängigkeit der Anschaffungs- und Betriebskosten. Dieser Ansatz führt nicht zu einer risikobasierten Cybersicherheit, hingegen zur Verschwendung von Ressourcen, die anderswo sinnvoller eingesetzt werden könnten. Cybersecurity ist das ganzheitliche Management von digitalen Risiken. Entsprechend müssen die Risiken identifiziert und analysiert sowie die Stärke der bestehenden Massnahmen bewertet werden. Aufgrund einer Risikostrategie werden Entscheide über weitere Massnahmen und Investitionen getroffen. Das Geld soll dort hinfliessen, wo es die Risiken am effektivsten und effizientesten entschärft und damit tragbar macht. Die Höhe der Budgetposten sollte die effektiven Risiken abbilden.

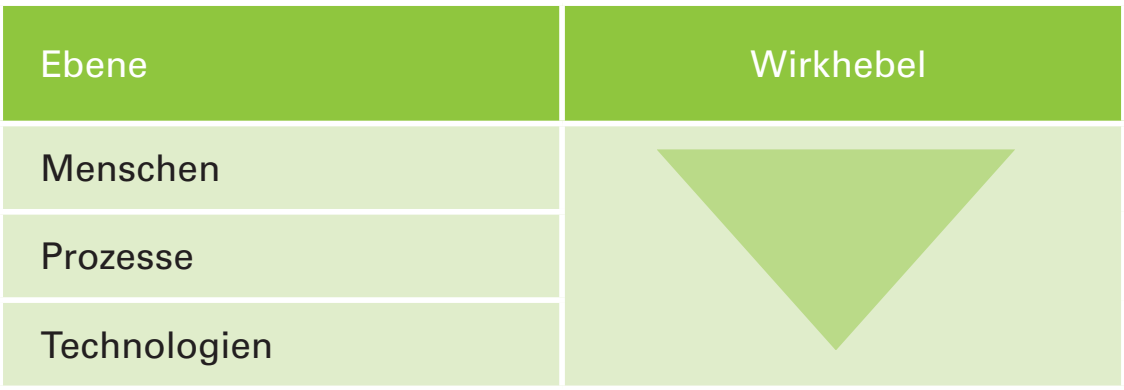

Abbildung 2: Wirkhebel von Sicherheitsmassnahmen

Technische Sicherheit skaliert nicht. Der Aufwand, um den technischen Grundschutz zu gewährleisten, ist für ein kleines Unternehmen mit 10 bis 50 Mitarbeitern nur unwesentlich kleiner als für ein grosses Unternehmen mit 250 bis 500 Mitarbeitern, da für eine kleine Infrastruktur grundsätzlich die gleichen technischen Grundschutzmassnahmen nötig sind. Daher ist es vor allem für kleinere Unternehmen wichtig, in Massnahmen zu investieren, die skalieren und einen grossen Wirkhebel haben. Die Wahrscheinlichkeit, dass sich ein Mitarbeiter Schadsoftware einfängt, die sich über das Netzwerk auf weitere Teile der Infrastruktur ausbreitet, ist bei einem grossen Unternehmen bei gleicher Sicherheitskompetenz der Mitarbeiter rein mathematisch gesehen wesentlich grösser als bei einem kleinen und tendiert nahezu gegen 100 Prozent. Daher lohnt es sich für kleine Unternehmen umso mehr, in die Sicherheitsschulung der Mitarbeiter zu investieren. Aber auch für alle anderen Unternehmen sind neben einer passenden, aktuellen Sicherheitstechnologie Investitionen in Prozesse und Menschen mindestens so wichtig. Mit klaren, verbindlichen Richtlinien und gezielter Schulung der Mitarbeiter (Endbenutzer und Administratoren) kann mehr bewirkt werden als nur mit technischen Lösungen alleine. Unabhängig von der Unternehmensgrösse muss ein digitaler Sicherheitsvorfall als unvermeidbares Risiko betrachtet werden. Entsprechend sind Investitionen auch in Entdeckungs- und Wiederherstellungsmassnahmen zwingend.

Richtgrössen für ein Cybersecurity-Budget

Ein Computerarbeitsplatz kostet in der Schweiz je nach Branche 2'500 bis 7'000 Schweizer Franken im Jahr. Darin sind sämtliche Kosten für Hardware, Software und Services für Arbeitsplatzrechner beziehungsweise Notebooks, Drucker, Server und Netzwerk sowie für Mitarbeiterschulung eingeschlossen. Dabei ist zu berücksichtigen, dass Mitarbeiter betreffend Cyber-Risiken und dem sicheren Umgang mit digitalen Arbeitsmitteln in der Praxis meist nur wenig bis gar nicht geschult werden.

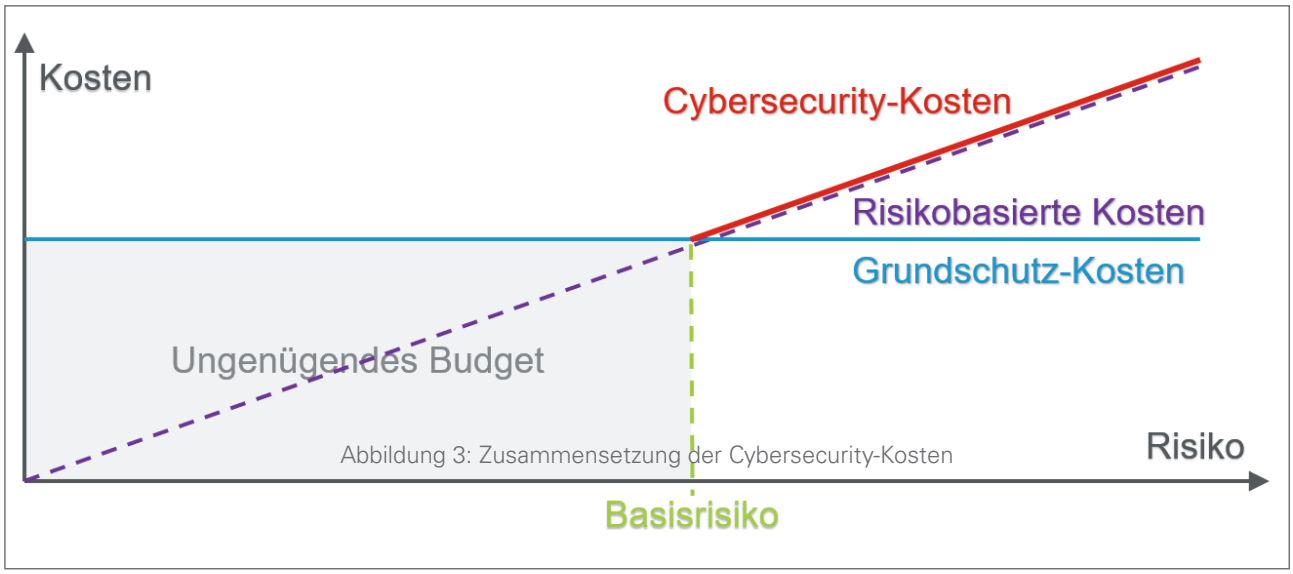

Abbildung 3: Zusammensetzung der Cybersecurity-Kosten

Generell sollte das Cybersecurity-Budget für den Grundschutz der IT mindestens ca. 15 bis 18 Prozent des IT-Budgets betragen. Auf einen Arbeitsplatz umgerechnet sind das mindestens 375 bis 1'000 Franken jährlich. Hinzu kommen die Kosten für allfällige spezifische Risiken durch individuelle Sicherheitsanforderungen. Diese Ausgaben betreffen lediglich die laufenden Kosten für Unternehmen auf einem ausreichenden Sicherheitsniveau. Die Investitionen für die Erreichung des entsprechenden Sicherheitsstandards fallen zusätzlich an. Als Faustregel sollte dieser Aufwand während der ersten 3 bis 5 Jahre das Ein- bis Zweifache des Grundschutzbudgets betragen. Damit kann in vernünftiger Frist ein risikogerechtes Sicherheitsniveau erreicht werden.

Diese Aufbaukosten umfassen insbesondere die Inventarisierung sämtlicher Hardware, Software, Daten und Dienste sowie deren Klassierung und Risikobewertung, die Ausarbeitung der Sicherheitsarchitektur mit zentraler Aufzeichnung aller sicherheitsrelevanten Ereignisse und zentraler Orchestrierung der Systeme, die Härtung von Systemen, die Zonierung des Netzwerks, den Aufbau eines Notfall-Managements mit Incident Response (Reaktion auf Vorfälle) und Disaster Recovery (Notfallwiederherstellung) und die Automatisierung der zeitkritischen und personalintensiven Security-Prozesse. Die entsprechenden Prozesse müssen soweit dokumentiert werden, dass sie von jedem Zuständigen verstanden und ausgeführt werden können. Und nicht zuletzt sollte mit Richtlinien und Schulung der Mitarbeiter eine Sicherheitskultur etabliert werden. Allgemein stellen die Kosten für Mitarbeiterschulung und Notfall-Management die grössten Brocken in einem Cybersecurity-Budget dar. Da die meisten Unternehmen kaum in der Lage sind, alle Aufgaben aus eigener Kraft zu stemmen, sind zusätzlich entsprechende Kosten für externe Berater und Integratoren einzurechnen.

Für eine Organisation mit 35 Mitarbeitern und Computerarbeitsplatzkosten von jährlich je 3'000 Franken sollte das Cybersecurity-Budget 15'750 Franken für laufende Kosten und ca. 26'250 Franken für Aufbaukosten und somit 42'000 Franken in den nächsten Jahren nicht unterschreiten. Daraus resultiert ein IT-Budget allein für die Computerarbeitsplätze von mindestens 131'250 Franken jährlich für die nächsten 3 bis 5 Jahre. Hinzu kommen die Kosten für Branchenlösungen, ERP, CRM, Web-Auftritt, Online-Shop, usw. mit einem Cybersecurity-Anteil für den Grundschutz von mindestens 10 bis 15 Prozent sowie die Kosten für die spezifischen Sicherheitsanforderungen, die über den Grundschutz hinausgehen. Letztere

können im Extremfall ein Mehrfaches der Grundschutzkosten betragen.

Die Cybersecurity für die Operational Technology (OT), d.h. die IT zur Steuerung von industriellen Prozessen, folgt grundsätzlich den gleichen Regeln wie für die IT, auch wenn es hier im Vergleich zur IT wesentliche Unterschiede betreffend der Risiken und Anforderungsprioritäten sowie der Möglichkeiten für den Schutz vor und die Erkennung von Cyber-Vorfällen bestehen. Die Individualität der Infrastrukturen, Altlasten mit langen Lebenszyklen und eine hohe Abhängigkeit von Lieferanten und Herstellern erschweren eine rasche risikobasierte Verbesserung der Cybersecurity. Entsprechend kompliziert, langwierig und individuell gestaltet sich die Budgetierung für die OT-Security. Daher können dazu keine sinnvollen Richtgrössen angegeben werden.

Budgetierung als Schlüsselelement der Cybersecurity

Wer glaubt, sich Cybersicherheit nicht leisten zu können oder müssen, muss es sich leisten können, die Kosten der Risiken zu tragen. Ein Geschäftsmodell, das digitalen Risiken ausgesetzt ist, ist ohne hinreichende Cybersicherheit nicht tragfähig. Sicherheit wird in vielen Bereichen als lästig und teuer empfunden. IT-Sicherheit sehen die viele Unternehmen lediglich als Schutz vor Hackern und daher als Aufgabe der IT. Dabei geht Cybersecurity über die reine IT-Sicherheit hinaus. Sie umfasst technische, organisatorische und rechtliche Massnahmen für die Schutzziele «Vertraulichkeit», «Integrität» und «Verfügbarkeit» sowohl von Hardware, Software, Daten als auch Services. Die grösste Schwachstelle ist jedoch der Mensch. In mehr als der Hälfte der Sicherheitsvorfälle im digitalen Bereich ist ein Mitarbeiter involviert – sei es als unachtsames Opfer, als Fehlbediener oder als willkürlicher Täter. Zudem sind Hardware und Software nie fehlerfrei und können sowohl Schäden durch Fehlfunktionen hervorrufen als auch durch einen technischen Defekt komplett zum Erliegen kommen. Es muss nicht immer ein Cyber-Angriff sein. Vor allem hinsichtlich der Verfügbarkeit ist es unerheblich, ob eine Komponente durch Hacker, durch eine Fehlbedienung oder durch einen technischen Fehler ausfällt.

1. Organisation	11. USB und externe Datenträger
2. Ziele, Strategie und Kennzahlen	12. Datenspeicherung und -übertragung
3. Asset Management	13. Backup und Restore
4. Risikoanalyse und Security Testing	14. Patch Management
5. Sicherheitsarchitektur	15. Visibilität und Entdeckung
6. Ausfallsicherheit und Redundanz	16. Überwachung und Alarmierung
7. Systemhärtung und -standardisierung	17. Notfall Management
8. Netzwerkzonierung	18. Richtlinien und Schulung
9. Identitäts- und Zugriffskontrolle	19. Lieferanten-Management
10. Fernzugriff	20. Budgetierung

Abbildung 4: Budgetierung als Schlüsselelement der Cybersecurity

Eine seriöse Cybersecurity-Strategie und -Budgetierung berücksichtigt all diese Faktoren. Richtig getätigte Investitionen stellen nicht nur den sorglosen Betrieb, sondern auch die Innovationsfähigkeit eines Unternehmens sicher. Digitalisierung hat ohne die nötige Cybersicherheit keine Zukunft und führt ein Unternehmen längerfristig ins digitale Verderben. Die IT-Infrastruktur bildet das Rückgrat eines Unternehmens und daher ist Cybersecurity ein wesentlicher Erfolgsfaktor in der digitalen Welt. Die Angst vor einer «Überdosierung an Sicherheit» ist fehl am Platz. Vielmehr sollte darauf geachtet werden, dass die Mittel optimal eingesetzt werden. Letzten Endes ist es unerheblich, wie die Cybersecurity-Kosten von den übrigen Kosten abgegrenzt werden. Entscheidend ist, dass genügend Budget bereitgestellt wird, um die Cyber-Resilienz eines Unternehmens sicherzustellen.

Zahlen und Fakten

Aktuelle Budgetentwicklungen

In den USA haben sich die Cybersecurity-Budgets gemäss den Zahlen des Online-Portals für Statistik Statista im Zeitraum von 2010 bis 2018 insgesamt um 141 Prozent erhöht. Das entspricht einer durchschnittlichen jährlichen Zunahme von 11.6 Prozent und dürfte in etwa auch auf die Schweiz zutreffen. Security-Anbieter gehen trotzdem von jährlichen Umsatzsteigerungen von 20 bis 30 Prozent aus. Sie beziehen sich dabei auf ein potenzielles Wachstum, welches auf der stetig steigenden Bedrohungslage und der wachsenden Vielfalt der angebotenen Sicherheitslösungen basiert. Die Budgets der Unternehmen können damit jedoch nicht Schritt halten. Tatsächlich klafft zwischen dem Marktangebot und der Inanspruchnahme eine Lücke.

Auch das Beratungsunternehmen EY kommt in seinem «Global Information Security Survey 2018-19» zum Ergebnis, dass die Budgets für die Cybersicherheit nicht mit jenen für die allgemeine Digitalisierung mithalten können und hier noch erheblicher Aufholbedarf besteht. Gemäss ihrer Studie weisen 77 Prozent der Unternehmen eine «limitierte Cyber-Resilienz» auf und wissen nicht einmal, was ihre kritischsten digitalen Schutzobjekte sind. Cybersecurity ist bei mehr als der Hälfte der Umfrageteilnehmer kein integraler Bestandteil der Unternehmensstrategie und der operativen Pläne. Die Absicht, mehr in eine zeitgemässe Cybersecurity zu investieren, liegt zwar im Trend, 87 Prozent der Unternehmen verfügen aber noch nicht über ein ausreichendes Budget, um das nötige Mass an Cybersicherheit und Widerstandsfähigkeit zu gewährleisten.

Risiken und ihre Wahrnehmung

Gemäss der Studie des Ponemon Institute von 2018, in der 477 Organisationen aus 15 Ländern untersucht wurden, verursachte eine einzelne Datenpanne einen Schaden von durchschnittlich 3.86 Millionen US-Dollar. In Deutschland lagen die durchschnittlichen Kosten einer Datenpanne mit 3.88 Millionen Euro etwas höher. Die Kosten einer Mega-Datenpanne mit mehr als einer Million betroffener Datensätze werden aktuell sogar mit 40 bis 350 Millionen US-Dollar beziffert und haben sich in den letzten fünf Jahren fast verdoppelt. Durchschnittlich betrug die Zeit zwischen einer Datenpanne und ihrer Entdeckung 197 Tage, während ihre Behebung durchschnittlich 69 Tage beanspruchte. Unternehmen, die eine Datenpanne in weniger als 30 Tagen eindämmen konnten, sparten über 1 Million US-Dollar im Vergleich zu solchen, die mehr als 30 Tage brauchten (3.09 Millionen Dollar gegenüber 4.25 Millionen Dollar im Durchschnitt).

Gemäss dem «Cybercrime Tactics and Techniques» Report vom August 2019 der Sicherheitsfirma Malwarebytes hat sich der Fokus von Cyber-Kriminellen in den letzten Monaten dramatisch verschoben. Infektionen mit Ransomware (Erpressungs-Trojaner) bei Unternehmen haben global im Vergleich zum Vorjahr um 365 Prozent zugenommen, während sie bei Privatpersonen stark rückläufig sind. Cyber-Kriminelle konzentrieren ihre Aktivität auf die lukrativsten Zielobjekte.

4 Prozent der Schweizer KMU werden jährlich Opfer von Ransomware und 36 Prozent werden von Malware wie Viren oder Trojanern befallen. Trotzdem beurteilen 56 Prozent den eigenen Schutz als gut bis sehr gut. Nur gerade 4 Prozent der Schweizer KMU erachten die Risiken von Cyber-Vorfällen als existenzgefährdend und 10 Prozent halten einen durch einen Cyber-Angriff verursachten kompletten eintägigen Betriebsunterbruch für möglich. Dies ergab 2017 die Befragung von Geschäftsführern 301 Schweizer KMU durch das Institut für Marktforschung GFS.

Gemäss Kriminalstatistik der polizeilich registrierten Straftaten 2018 beträgt die Wahrscheinlichkeit, als Privatperson in der Schweiz innerhalb eine Jahres Opfer eines Einbruchdiebstahls zu werden, bescheidene 0.38 Prozent. In den USA liegt diese bereits bei 1.7 Prozent. Dagegen schätzt das Ponemon Institute, dass die Wahrscheinlichkeit, als Unternehmen innerhalb eines Jahres Opfer einer Datenpanne zu werden, aktuell mehr als 25 Prozent beträgt. Gemäss der GFS-Umfrage Anfang 2019 bei Privatpersonen, war bereits jeder Siebte schon einmal Opfer eines Cyber-Angriffs. Trotzdem ist mehr als die Hälfte der Befragten der Meinung, gut informiert zu sein und sich gegen solche Angriffe schützen zu können. Es ist tatsächlich nicht einfach, Risiken richtig einzuschätzen. Statistiken und Wahrnehmungen können stark voneinander abweichen. Dies ist ganz besonders bei Cyber-Risiken der Fall.

Auswirkungen der Europäischen Datenschutz-Grundverordnung

Viele Unternehmen, die von der Europäischen Datenschutz-Grundverordnung (DSGVO) betroffen sind, haben bereits erhebliche Investitionen getätigt, um die Einhaltung der neuen Richtlinien sicherzustellen, die seit dem 25.05.2018 verbindlich sind. Die DSGVO gilt auch für alle Unternehmen von Drittstaaten, die eine Niederlassung in der EU haben. Aufgrund des Marktortprinzips findet das Gesetz auch für viele Schweizer Unternehmen Anwendung, die Waren oder Dienstleistungen in der EU anbieten. Betroffene Unternehmen müssen neben angemessenen Sicherheitsmassnahmen der Dokumentationspflicht nachkommen, Einwilligungen zur Datenverarbeitung einholen und eine Datenschutzfolgeabschätzung durchführen sowie einen Datenschutzbeauftragten und, falls sie in der Union keine Niederlassung haben, einen Vertreter in der Union benennen. Zudem müssen sie in der Lage sein, ihre Compliance nachzuweisen. Bei Zuwiderhandlung gegen die DSGVO drohen empfindliche Bussen.

Mittlerweile wurden auch schon erste Bussen gegen fehlbare Unternehmen verhängt. Die erst kürzlich ausgesprochenen Strafgelder gegen die spanische Fussballiga (250'000 Euro) und vor allem gegen British Airways (204 Millionen Euro) sowie die Hotelkette Marriott (110 Millionen Euro) lassen darauf schliessen, dass das Gesetz nötigenfalls auch mit aller Härte durchgesetzt wird. Die DSGVO wird in den betroffenen Unternehmen mittelfristig zu höheren Ausgaben für den Datenschutz führen.

www.electrosuisse.ch