Studie zur Cybersicherheit

IT-SECURITY ALS WEGBEREITER

Wie schätzen Unternehmen ihr Risiko für Cyberangriffe ein? Wie investieren sie in die IT-Sicherheit und welche Rolle spielt diese in Geschäftsmodellen? Eine neue Studie von Mindfacts und BIGS im Auftrag von Trend Micro bringt überraschende Ergebnisse ans Licht. Die wichtigste Erkenntnis: Cybersecurity gilt nicht länger als Hindernis, sondern wird zum Wegbereiter für die Digitalisierung und Geschäftsentwicklung.

INHALTSVERZEICHNIS

VORWORT

Von Dr. Tim Stuchtey, Geschäftsführender Direktor des Brandenburgischen Instituts für Gesellschaft und Sicherheit (BIGS)

Die Bedrohung im Cyberraum steigt stetig an. Cyberkriminalität ist ein profitables Geschäftsmodell, hinzu kommen skrupellose und ressourcenstarke staatliche Akteure, die deutschen Unternehmen und der Volkswirtschaft Schaden zufügen wollen. Stellt man jedoch diesen Bedrohungen einen adäquaten Schutz der eigenen Netze und Systeme entgegen, muss die Sicherheit, trotz steigender Bedrohung, nicht leiden. Dass ein solider Schutz dafür aber unabdingbar ist, lernen viele erst, wenn sie einmal Opfer eines Angriffs geworden sind. Dann nämlich merken sie, dass der Schaden und die nachfolgenden Kosten um ein Vielfaches höher sind als die mit der Absicherung verbundenen Kosten. Immerhin reicht den meisten, einmal Opfer zu werden, um diese Lektion zu lernen. Schließlich steigt die Wahrscheinlichkeit eines erneuten Angriffs gerade bei den „populären" Ransomware-Attacken.

Ebenso positiv zu bewerten ist, dass unter den Befragten vermehrt die Sensibilität besteht, dass mit der Digitalisierung des eigenen Wertschöpfungsprozesses auch eine adäquate Absicherung erfolgen muss. Die Schutzmaßnahmen müssen in dem Maß zunehmen, wie der Angriffsvektor durch die Digitalisierung im Unternehmen steigt.

Viele der in dieser Studie befragten großen Mittelständler gehen gar einen Schritt weiter. Für sie ist Cybersicherheit nicht nur ein Thema, um sich vor den Schadenskosten eines Angriffs zu schützen. Sie versuchen IT-Sicherheit auch in den Wertschöpfungsprozess ihres Unternehmens zu integrieren und damit ihren Kunden einen Mehrwert zu bieten. Das damit einhergehende Leistungsversprechen, auch in turbulenten Zeiten zu liefern, ist ein Thema, das nicht nur in der Politik nach der Zeitenwende eine Rolle spielt. Zur Absicherung der Lieferketten gehört eben auch, bei Dienstleistern und Zulieferern darauf zu achten, dass diese ein zum eigenen Unternehmen passendes Resilienzniveau haben.

Viele, die die nachfolgende Studie lesen, werden in der Öffentlichkeit oder im eigenen Unternehmen als Experten bezeichnet. Als Experten haben wir ein vertiefendes Wissen in einem oder vielleicht einigen bestimmten Themenbereich(en). Mit voranschreitender Arbeitsteilung, auch und gerade im Bereich der Digitalisierung, fällt es schwer, alle Bereiche in der notwendigen Tiefe zu überblicken. Daher hat es mich gewundert, dass gerade bei den befragten Führungskräften der IT-Sicherheit, eine ausgeprägte Skepsis gegenüber externen Dienstleistern vorherrschend zu sein scheint. Für mich ist es offensichtlich, dass mittelständische Unternehmen nicht in allen Eventualfällen die notwendige Expertise im Haus haben können. Sollten sie aus wirtschaftlicher Vernunft heraus auch nicht. Vielmehr ist es wichtig, die Expertise zu besitzen, die richtigen Dienstleister für die anstehenden Herausforderungen zu identifizieren.

1. MANAGEMENT SUMMARY

Fast die Hälfte der Unternehmen in Deutschland (45 Prozent) waren in den vergangenen 24 Monaten von einem Cyberangriff betroffen, so eine aktuelle Studie des Marktforschungsinstituts Mindfacts im Auftrag von Trend Micro. Befragt wurden 300 Führungskräfte aus der IT und IT-Security in Unternehmen mit mehr als 250 Mitarbeitern aus verschiedenen Branchen. Am häufigsten wurde der Dienstleistungssektor attackiert (52 Prozent), gefolgt vom produzierenden Gewerbe (46 Prozent) und dem Handel (20 Prozent). Dabei fällt auf, dass Cyberkriminelle ihre Opfer häufig ganz gezielt auswählen. 57 Prozent der Betroffenen geben an, dass sich der Angriff speziell gegen ihr Unternehmen richtete und kein Zufallstreffer einer breit angelegten Kampagne war. Wie wirkt sich die aktuelle Bedrohungslage auf das Risikobewusstsein und Investitionen in die IT-Sicherheit aus? Und welche Rolle spielt die Cybersecurity in Geschäftsmodellen? Das ermittelte das Brandenburgische Institut für Gesellschaft und Sicherheit (BIGS) anhand der Mindfacts-Daten. Die zentralen Ergebnisse der Auswertung:

- Strategisches Investment in IT-Security zahlt sich aus. Unternehmen, die Cybersicherheit als Beitrag zur Wertschöpfungskette sehen, investieren proaktiv in Security. Ebenso Unternehmen, die schon einmal Erfahrung mit Cyberangriffen gemacht haben.
- Security wird zum Enabler für die Digitalisierung. 76 Prozent der Unternehmen betrachten IT-Sicherheit als wichtig für die Wirtschaft. 65,7 Prozent möchten Digitalisierungsprojekte durch Modernisierung der IT-Sicherheit vorantreiben.
- Der Nutzen von externen Experten wird oft noch verkannt.

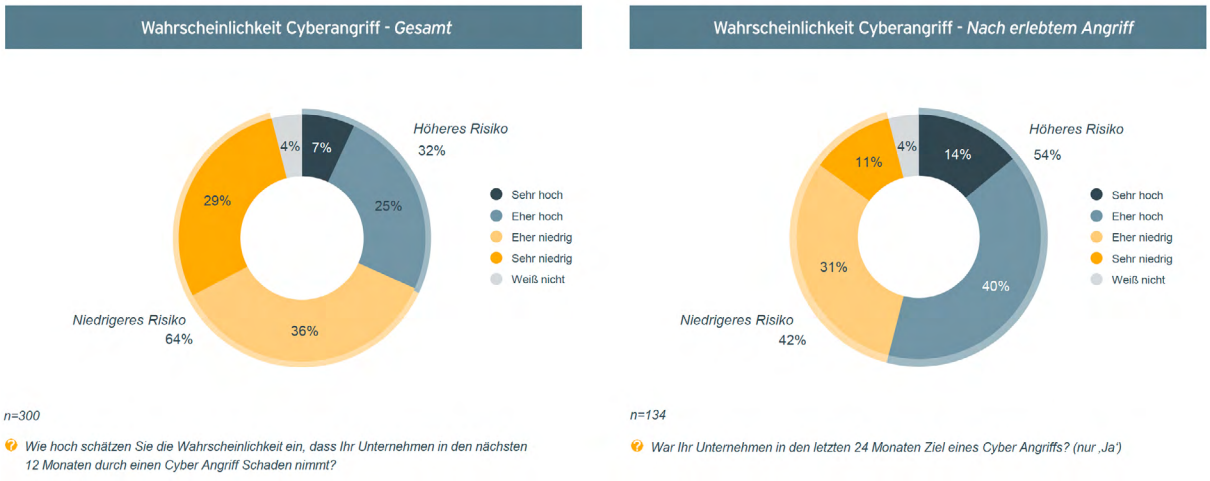
2. STRATEGISCHES INVESTMENT IN IT-SECURITY ZAHLT SICH AUS

2.1. Risikobewusstsein steigt mit der Erfahrung

Viele der Befragten unterschätzen noch die Gefahr, der sie ausgesetzt sind. Nur knapp ein Drittel (32 Prozent) hält es für eher wahrscheinlich, dass ihr Unternehmen in den nächsten zwölf Monaten Schaden durch einen Cyberangriff nehmen wird. Unter den IT-Security-Experten ist die Awareness deutlich höher: 49 Prozent von ihnen erachten das Schadensrisiko als hoch oder sogar sehr hoch. Grundsätzlich steigt das Risikobewusstsein mit der Erfahrung. 54 Prozent der Unternehmen, die in den vergangenen 24 Monaten Opfer eines Cyberangriffs waren, haben Sorge, erneut angegriffen zu werden. Diese Angst ist durchaus berechtigt: Studien zeigen, dass mehrfache Attacken auf dasselbe Unternehmen häufig vorkommen. Insbesondere, wer schon einmal von einem Ransomware-Angriff betroffen war und Lösegeld gezahlt hat, gilt in der cyberkriminellen Szene als attraktives Ziel. 80 Prozent dieser Unternehmen wurden ein zweites Mal angegriffen, oftmals mit höherer Erpresserforderung . Es lohnt sich also, auch nach überstandenem Cybervorfall aufmerksam zu bleiben. Um sich zu schützen, ist es wichtig, das Security-Konzept kontinuierlich an aktuelle Anforderungen anzupassen. Entscheidend sind sowohl starke präventive Maßnahmen zur Angriffsabwehr als auch eine leistungsfähige Detection und Response über alle Ebenen der IT-Umgebung hinweg.

Schaden durch Cyberangriff in den nächsten 12 Monaten - Gesamt und nach erlebtem Angriff

Insgesamt sehen nur 32% eine höhere Wahrscheinlichkeit, angriffserfahrene Unternehmen sind mit 54% skeptischer.



2.2. Leiderprobte Unternehmen investieren strategisch

Wer schon einmal Opfer eines Cyberangriffs war, musste sich intensiver mit IT-Sicherheit beschäftigen. In dieser Gruppe ist der Anteil der Unternehmen, die strategisch in Cybersecurity investieren, mit 70 Prozent besonders hoch. Unter denen, die Schäden durch künftige Attacken für wahrscheinlich halten, sind es sogar 74 Prozent. Ein strategisches Investment bedeutet präventives, proaktives Verhalten. Unternehmen mit geringerem Risikobewusstsein geben dagegen eher reaktiv Geld für Security aus, um kurzfristig Sicherheitsprobleme zu lösen. Grundsätzlich sind die Investitionen in die Cybersicherheit in fast allen Branchen in den vergangenen 24 Monaten gestiegen. Gerade bei kleineren und mittleren Unternehmen entscheidet häufig die Geschäftsführung über die Ausgaben . Security-Verantwortliche stehen daher vor der Herausforderung, die Notwendigkeit ihrer Vorhaben überzeugend darzulegen.

2.3. Prävention spart Geld

Betrachtet man die Entwicklung der vergangenen Jahre, zeigt sich klar, dass präventive, strategische Ausgaben für Cybersecurity kostengünstiger sind als ein reaktives Vorgehen. Laut einer Bitkom-Studie ist nicht nur die Zahl der Cyberangriffe gestiegen, sondern auch die Schadenssumme. Letztere hat sich 2022 im Vergleich zu 2017 verdreifacht . Einen Cybervorfall zu bewältigen, kann sehr teuer werden. 39 Prozent der Betroffenen mussten Mitarbeiter aus den Bereichen Recht, Finanzen und Management hinzuziehen, 35 Prozent mussten externe Berater beauftragen . Dazu kommen Kosten für Ausfallzeiten, Datenverlust, Reputationsschäden, Wiederherstellung der Systeme und rechtliche Aspekte. Eine gute Vorsorge kann im Vergleich dazu viel Geld sparen und ist daher ein wichtiger Teil einer umfassenden Cybersicherheitsstrategie.

3. IT-SECURITY WIRD ZUM ENABLER FÜR DIE DIGITALISIERUNG

3.1. Digitalisierungsaffine Unternehmen sind risikobewusster

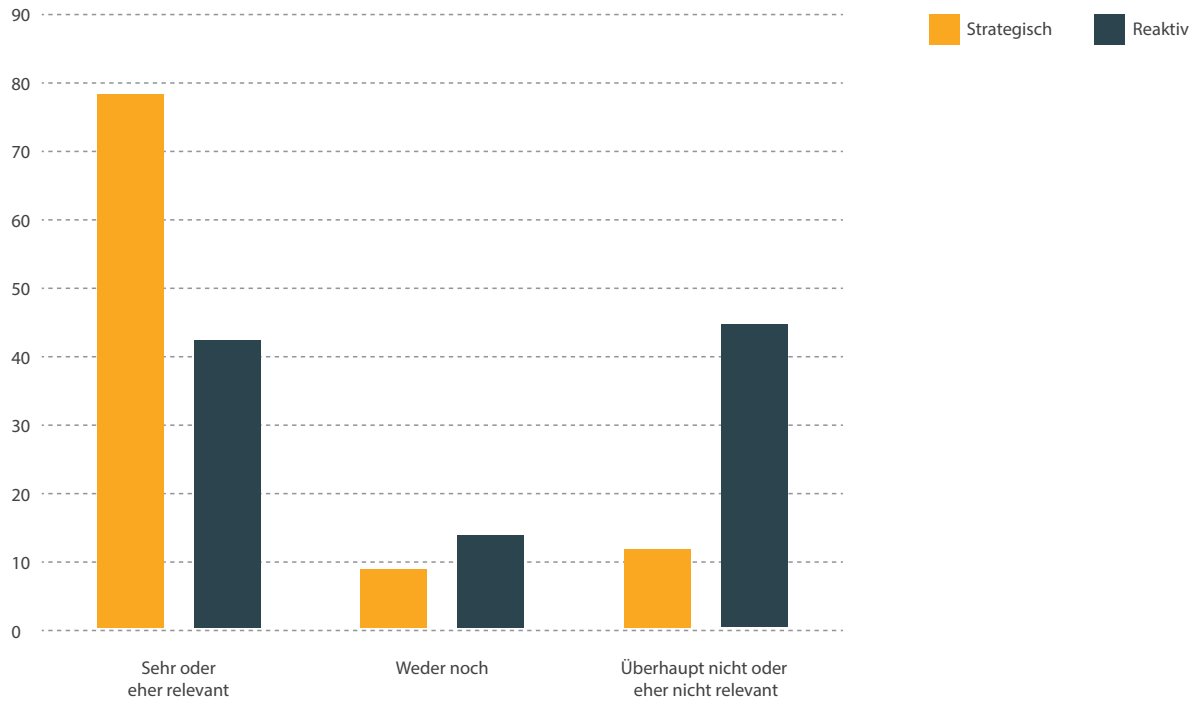
Sich vor Cyberangriffen zu schützen, sichert die Geschäftsfähigkeit und ist damit aus ökonomischer Sicht unverzichtbar. Die Mehrheit der deutschen Unternehmen (76 Prozent) erachtet die IT-Sicherheit als wichtig für die Wirtschaft. Nur 13,7 Prozent sehen sie als weniger relevant an. Diejenigen, die die strategische Bedeutung von Cybersicherheit erkennen, nehmen Bedrohungen im Cyberraum ernster. Insbesondere digitalisierungsaffine Unternehmen haben eine größere Awareness: Sie sind sich der Gefahren, welche die zunehmende Vernetzung bringt, bewusst und wissen daher, wie wichtig die Absicherung ist. Nur acht Prozent der Studienteilnehmer sehen kein erhöhtes Risiko durch die Digitalisierung, aber erschreckende 14,3 Prozent sind sich noch unschlüssig. Wie gefährlich diese Unbedarftheit ist, zeigt ein Blick auf den Digitalisierungsschub während der Pandemie: Laut einer Bitkom-Studie hat die Corona-bedingte Verlagerung von Arbeitsplätzen ins Home Office bei 59 Prozent der Unternehmen zu einem Anstieg von Cybervorfällen geführt und bei mehr als der Hälfte der Betroffenen Schaden verursacht .

3.2. IT-Security ist wirtschaftlich profitabel

Insgesamt überwiegt bei den Befragten das Bewusstsein, dass Security eine wichtige Voraussetzung für die Digitalisierung und Entwicklung neuer Geschäftsmodelle bildet. Zwei Drittel (66 Prozent) wollen Digitalisierungsprojekte durch Modernisierung der IT-Sicherheit vorantreiben. Dabei gibt es einen Zusammenhang zwischen einem präventiven Ansatz und Innovationen: 79 Prozent der Unternehmen, die strategisch in Security investieren, halten dies für relevant, um neue Geschäftsmodelle zu entwickeln. 64 Prozent sagen zudem, dass IT-Security einen Mehrwert für den Kunden bringt. Unternehmen betrachten IT-Sicherheit folglich nicht mehr nur als Herausforderung, sondern als wirtschaftlich profitabel. Denn Cybersecurity ermöglicht Innovationen, eröffnet neue Geschäftsfelder und lässt sich gewinnbringend in das eigene Geschäftsmodell integrieren. Strategische Investitionen in IT-Sicherheit lohnen sich daher für die Geschäftsentwicklung und sind wichtig, um Kundenerwartungen zu erfüllen.

Investitionsverhalten und Entwicklung neuer Geschäftsmodelle

79% der befragten Unternehmen, die strategisch investieren, erachten innovative Geschäftsmodelle mit Hilfe von IT-Sicherheit auch als bedeutsamer. 44% der Unternehmen, die weniger Bedeutung in innovativen Geschäftsmodellen mit IT-Sicherheit sehen, investieren eher reaktiv.

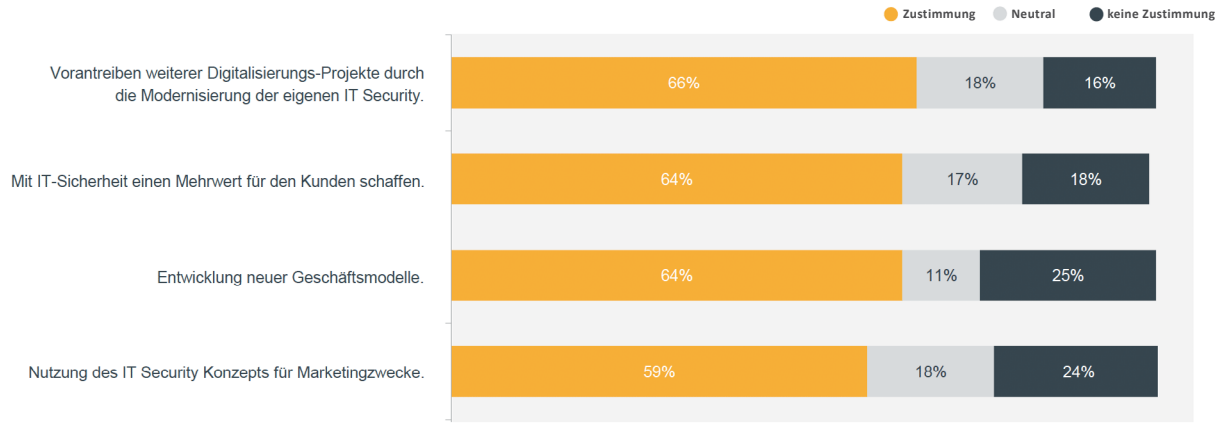


3.3. Fehlende Cybersecurity schadet der Reputation

Bei Kunden wächst das Bewusstsein für Cybersecurity. Daher erwarten sie von Unternehmen angemessene Sicherheitsmaßnahmen. Fehlen diese, wirkt sich das rufschädigend aus. So hatten 30 Prozent der Unternehmen, die Opfer eines Cyberangriffs waren, mit Kundenverlust zu kämpfen . Der Schaden, der aus dem Reputationsverlust resultiert, kann deutlich höher sein als die Kosten, die für strategische IT-Sicherheit anfallen . Auch vor diesem Hintergrund lohnt es sich also, präventiv in Cybersecurity zu investieren und auf diese Weise ein positives Marken-Image aufzubauen. Die Mehrheit der Befragten hat das erkannt: 59 Prozent nutzen ihr IT-Security-Konzept bereits für Marketingzwecke.

Einfluss der IT Security auf Geschäftsmodelle - Gesamt

37% halten das Vorantreiben weiterer Digitalisierungs-Projekte für sehr relevant



n=300

Welche Rolle spielt die IT Security im Rahmen der Geschäftsmodelle Ihres Unternehmens?

4. DER NUTZEN VON EXTERNEN EXPERTEN WIRD NOCH VERKANNT

4.1. Hohes Vertrauen in die eigenen Fähigkeiten

Die BIGS-Auswertung zeigt, dass sich Unternehmen der zunehmenden Bedeutung von Cybersecurity sowohl für die Schadensvermeidung als auch für die Geschäftsentwicklung bewusst sind. Aber wer entwickelt das Security-Konzept und wer soll es umsetzen? Interne IT-Security-Teams haben hier großes Vertrauen in ihre eigenen Fähigkeiten. Nur 14,7 Prozent der Befragten aus der IT-Sicherheit erachten es als notwendig, mit externen Experten zusammenzuarbeiten. Ganz anders sehen das die Kollegen aus dem IT-Bereich: 56,9 Prozent von ihnen sehen den Bedarf nach externen Experten. Möglicherweise lassen sich IT-Security-Mitarbeiter nur ungern von außen in ihren Arbeitsbereich reinreden. Vielleicht haben sie auch in der Vergangenheit schlechte Erfahrungen mit externen Beratern gemacht oder erachten es als sinnlos, Geld für Managed Services auszugeben.

4.2. Selbstüberschätzung kann gefährlich sein

Tatsächlich birgt diese Skepsis gegenüber externen Dienstleistern aber auch Gefahren. Denn wenn sich interne IT-Security-Teams selbst überschätzen, entstehen Sicherheitslücken. In der Praxis wird es immer schwieriger, die wachsenden Anforderungen an die IT-Sicherheit ohne die Hilfe von externen Spezialisten zu erfüllen. Nicht nur Cyberangriffe, sondern auch IT-Umgebungen und Security-Technologien werden immer komplexer. Es reicht nicht aus, in führende Sicherheitslösungen zu investieren. Man muss sie auch richtig konfigurieren, managen, rund um die Uhr monitoren und die Warnmeldungen der Systeme analysieren. Außerdem ist eine kontinuierliche Risikobewertung erforderlich. Nur wenige Unternehmen haben dafür ausreichend Personal und Expertise. Weltweit fehlen 3,4 Millionen Fachkräfte für Cybersecurity, so die aktuelle ISC Workforce Study . 74 Prozent der Unternehmen sehen sich dadurch moderat bis extrem gefährdet.

4.3. Vorteile von Managed Security Services

IT-Sicherheitsverantwortliche sollten ihre Zurückhaltung gegenüber Managed Security Services überdenken. Zwar schrecken mitunter der Preis und ein möglicher Kontrollverlust über die IT-Sicherheit manche Unternehmen ab, den digitalen Schutz des Unternehmens an einen externen Dienstleister abzugeben. Die Zusammenarbeit mit externen Spezialisten bringt jedoch, eine gründliche Planung und Integration vorausgesetzt, Vorteile mit sich:

- Managed Services Provider (MSPs) entlasten das interne Team.
- Eigene Mitarbeiter können sich auf ihre Kernaufgaben konzentrieren.
- Unternehmen können die Ressourcen jederzeit nach Bedarf abrufen.
- Die externen Spezialisten sind 24/7 verfügbar.
- Unternehmen profitieren von aktuellem Expertenwissen, ohne dass sie es selbst aufbauen müssen.
- Spezialisierte Security-Analysten kennen neueste Angriffsmuster, globale Zusammenhänge und können unternehmensübergreifend Bedrohungen erkennen.
- Im Falle eines Cyberangriffs helfen die Experten, Schaden zu minimieren und schnell wieder betriebsfähig zu werden.

4.4. Potenzial von Pay-as-you-go-Modellen bleibt oft noch ungenutzt

Viele MSPs bieten ihre Leistungen mittlerweile im Pay-as-you-go-Modell an, sodass Unternehmen nur für das zahlen, was sie auch tatsächlich nutzen. Ohne hohe Startinvestitionen profitieren sie von moderner Security-Technologie. Statt CapEx fallen OpEx an, sodass weniger Kapital gebunden wird und mehr Budget für weitere IT Security-Maßnahmen bleibt. Bisher haben nur etwas mehr als die Hälfte (56 Prozent) der IT-Security-Führungskräfte das Potenzial von Pay-as-you-go-Modellen erkannt. Unter den Befragten aus dem Bereich IT sind es sogar nur 34 Prozent. Insgesamt ist sich fast ein Drittel der Studienteilnehmer unschlüssig, ob Pay-as-you-go in der IT-Sicherheit finanzielle Vorteile bringt. Hier fehlen möglicherweise noch Kenntnisse. Grundsätzlich haben jedoch Unternehmen aller Branchen und Größen Interesse an diesem Bezahlmodell.

5. FAZIT

Die BIGS-Studie zeigt: Je mehr Erfahrung Unternehmen mit IT-Security und Cybervorfällen haben, umso besser können sie Risiken einschätzen und umso eher investieren sie strategisch in die IT-Sicherheit. Ein solches präventives Vorgehen lohnt sich, denn die Kosten, die durch einen Cyberangriff entstehen können, übersteigen die Ausgaben für vorbeugende Security-Maßnahmen meist erheblich. Viele Unternehmen haben mittlerweile erkannt, dass sich Investitionen in die IT-Sicherheit auch wirtschaftlich auszahlen. Cybersecurity schafft die Voraussetzung für Digitalisierungsprojekte und neue Geschäftsmodelle, bringt einen Mehrwert für Kunden und lässt sich für Marketing-Zwecke einsetzen. IT-Sicherheit wird damit zum Wegbereiter für die Digitalisierung und Geschäftsentwicklung. Bei der Umsetzung kann es sich lohnen, mit externen Experten zusammenzuarbeiten und auf ein Pay-as-you-go-Modell zu setzen. So können Unternehmen dem Fachkräftemangel trotzen, ein hohes Sicherheitsniveau erreichen und ihre Ressourcen optimal nutzen

Über das BIGS:

Das Brandenburgische Institut für Gesellschaft und Sicherheit (BIGS) ist ein unabhängiges, überparteiliches und nicht-gewinnorientiertes Institut in Potsdam mit der Mission, durch eigene anwendungsorientierte Forschung, Analysen, Veröffentlichungen und Veranstaltungen Fragen und Herausforderungen ziviler Sicherheit zu begegnen und Brücken zwischen Theorie und Praxis zu schlagen. Das Institut soll einen Beitrag dazu leisten, die Interdisziplinarität des Problems „Sicherheit“ zu reflektieren, entsprechend zu analysieren und so dazu beizutragen, dass wissenschaftliche Erkenntnisse umfassend berücksichtigt werden, wenn sich der Staat, die Gesellschaft und die Wirtschaft Herausforderungen ziviler Sicherheit stellt.

Über Trend Micro:

Bei Trend Micro ist es unser Ziel, die Welt für den Austausch digitaler Informationen sicherer zu machen. Wir sind davon überzeugt, dass Cyberrisiken gleichzeitig Geschäftsrisiken darstellen. Deshalb ermöglichen wir Unternehmen vollständige Transparenz und Kontrolle ihrer digitalen Assets. So verstehen sie, wie gut sie geschützt sind und welche Investitionen wichtig sind, um das Risiko zu senken.

Mit uns wird die Welt sicherer, da wir schon früh erkennen, wie sich moderne Infrastrukturen, Nutzerverhalten, Applikationsentwicklung und damit auch Cyberbedrohungen verändern und darauf reagieren.