Security Awareness Trainings im deutschen **Mittelstand –** Sind **Mitarbeiter Teil** der **Cyberabwehr?**

INHALT

ERGEBNISSE AUF EINEN **BLICK**

50% der befragten Mittelständler waren bereits von **IT-SECURITY-VORFÄLLEN** betroffen, die durch das fehlerhafte Verhalten der Angestellten ausgelöst wurden.

ACHT von ZEHN UNTERNEHMEN

führen Security-Awareness-Maßnahmen für ihre Mitarbeiter durch.

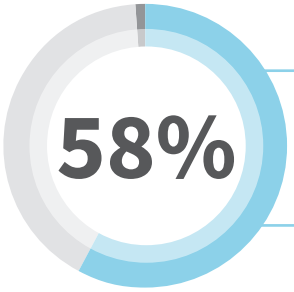
ACHT von ZEHN MITTELSTÄNDLERN

setzen bei Security Awareness Trainings auf Wiederholungen.

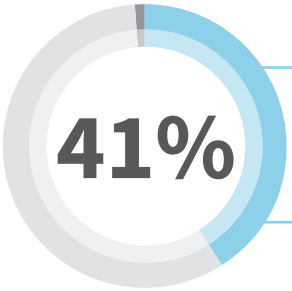
Die **INVESTITION IN SECURITY-SCHULUNGSMAßNAHMEN** lohnt sich:

87 PROZENT

der befragten Unternehmen erzielten positive Effekte, zum Beispiel einen umsichtigeren Umgang mit den **IT-RESSOURCEN.**



der Unternehmen bevorzugen Präsenzveranstaltungen



der Mittelständler setzen auf E-Learning-Angebote

Das wichtigste Thema für den Mittelstand bei **SECURITY AWARENESS TRAININGS** ist

„SICHERHEITS-VORFÄLLE“

das bedeutet Angriffe zu erkennen und im Ernstfall richtig zu reagieren.

Unternehmen des deutschen Mittelstandes sind beliebte Ziele für Cyberattacken. Dabei sind nicht nur ungepatchte Sicherheitslücken entscheidend für den Erfolg der Angreifer, ein wesentliches Kriterium ist der Faktor Mensch. Die aktuelle Umfrage im deutschen Mittelstand von G DATA CyberDefense zeigt: Die Hälfte der Untenehmen konnte Security-Vorfälle, zum Beispiel eine Malware-Infektion des Netzwerkes, konkret auf das fehlerhafte Verhalten von Mitarbeitern zurückführen.

Security Awareness Trainings verhindern erfolgreiche Cyberangriffe, weil Mitarbeiter mit dem nötigen Fachwissen ausgestattet werden und so zu einem Teil der unternehmerischen Cyberabwehr werden. Ein gut geschulter Angestellter weiß, was im Fall eines Cyberangriffs zu tun ist und verhindert durch sein umsichtiges Handeln größere Schäden. Die Vorteile liegen auf der Hand. Wie steht aber der deutsche Mittelstand zu diesem wichtigen Thema der IT-Sicherheit? Werden die Mitarbeiter mit in die Cyberabwehr eingebunden und ist die Maßnahme wirksam?

DER MITARBEITER ALS TÜRÖFFNER FÜR CYBERKRIMINELLE

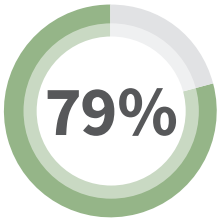
Die sorgfältige Aufarbeitung eines erfolgreichen Angriffs in einem Unternehmen ist wichtig, um zu verstehen, was bei dem Vorfall passiert ist und warum dieser erfolgreich war. Wie eingangs bereits dargestellt, sind bei 50 Prozent der befragten Mittelständler falsche Handlungen von Angestellten entscheidend für das Durchdringen einer Attacke gewesen. Stammt der Umfrageteilnehmer aus dem IT-Umfeld, wird dieser Sachverhalt häufiger festgestellt, als wenn der Befragte aus dem Bereich Personal kommt.

In der Regel nutzen Cyberkriminelle Phishing-Mails als Angriffsvektor, um ein Unternehmensnetzwerk zu infiltrieren. In einigen Fällen sind dies gezielte Aktionen, in anderen Fällen basieren die Attacken auf breit angelegten Kampagnen. Mitarbeiter fallen auf solche Nachrichten leicht herein. Security Awareness Trainings machen Angestellte sicher im Umgang mit Phishing und anderen Bedrohungen und verhindern so erfolgreiche Angriffe.

KLEINERE UNTERNEHMEN HABEN NACHHOLBEDARF

Acht von zehn Unternehmen im Mittelstand (79 Prozent) führen Schulungen für ihre Mitarbeiter durch.

Hierbei zeigt sich: Je größer die Belegschaft, desto höher ist der Anteil der Firmen, die diese einsetzen. 90 Prozent der Unternehmen mit 501 bis 1.000 Mitarbeitern setzen auf Trainings, dagegen beträgt der Anteil bei Unternehmen mit bis zu 99 Mitarbeitern knapp 70 Prozent. Mit der steigenden Anzahl der Mitarbeiter wächst auch generell das Risiko, dass Angestellte eine Cyberattacke auslösen könnten. Grundsätzlich stehen alle Firmen im Fokus der Cyberkriminellen, denn Unternehmen verfügen über interessante Informationen, die sich zu Geld machen lassen. Darunter fallen beispielsweise Kundendatenbanken, diese eignen sich für die Erpressung von Lösegeld für verschlüsselte IT-Segmente mit Hilfe von Ransomware.



führen Schulungen
für ihre Mitarbeiter durch

Bei dieser Fragestellung wird deutlich, dass IT-Sicherheit stark abhängig vom Jahresumsatz ist: Bei den Unternehmen mit einem Jahresumsatz bis zu einer halben Million Euro setzt nur ein Drittel auf Security Awareness Trainings. Hier besteht ein dringender Nachholbedarf. Fraglich ist allerdings, ob das nötige Budget tatsächlich nicht vorhanden ist oder Verantwortliche stattdessen falsche Prioritäten bei der Planung setzen. Oft gibt es kein eigenes Budget für IT-Sicherheit, es ist lediglich ein Teil des gesamten IT-Etats.

Ein Blick auf die Position der Umfrageteilnehmer zeigt: 93 Prozent der Chief Information Security Officers (CISOs, IT-Leiter und IT-Security-Beauftragte) antworten, dass in ihrem Unternehmen Security Awareness Trainings für die Mitarbeiter durchgeführt werden. Diese Fachkräfte können den Nutzen und die Wirksamkeit gut einschätzen und die Ursachen für das Durchdringen einer Cyberattacke in die IT-Systeme nachvollziehen. Stammt die befragte Person aus dem Personalbereich, zeigt sich ein anderes Bild: Nur 60 Prozent nutzen diese Trainingsmaßnahme.

der Chief Information Security
Officers antworten, dass Security
Awareness Trainings durchgeführt
werden

KEINE AWARENESS-SCHULUNGEN AUFGRUND FATALER DENKWEISE

Während die Mehrheit des deutschen Mittelstandes auf Security Awareness Trainings setzt, führen zwei von zehn Unternehmen keine Schulungsmaßnahmen für ihre Mitarbeiter durch. 47 Prozent dieser Befragten begründen dies damit, dass sie bei der IT-Sicherheit bereits gut aufgestellt seien. Trainings erscheinen ihnen daher nicht notwendig. Besonders auffällig: 60 Prozent der befragten IT-Leiter, CISOs und IT-Security-Beauftragten in den Unternehmen, die keine Schulungsmaßnahmen anbieten, antworten so. Das Problem: Die betroffenen Mittelständler sind vielleicht auf der technischen Ebene gut aufgestellt, aber ihre IT-Sicherheit ist trotzdem lückenhaft. Der Faktor Mensch ist ein entscheidendes Kriterium bei der Abwehr von Cyberangriffen, daher ist diese Denkweise grob fahrlässig und fatal. Im Lagebild Wirtschaftsschutz NRW 2019 zeigt sich deutlich, dass einige Unternehmen wenig Wert auf Schulungs- und Sensibilisierungsmaßnahmen legen. Dabei geben die Autoren der Studie die dringende Handlungsempfehlung heraus, die Sensibilisierung des Führungspersonals und aller Mitarbeiter in Unternehmen für Cybergefahren konsequent voranzutreiben.

der Unternehmen führen keine Schulungsmaßnahmen für ihre Mitarbeiter durch

Ein Blick auf die Gründe, warum mittelständische Unternehmen keine Security Awareness Trainings durchführen zeigt: Ein Viertel verfügt nach eigenen Angaben nicht über das notwendige Budget. Dies bedeutet, dass Mitarbeiter-Schulungen eine Option sein könnten, wenn die nötigen finanziellen Mittel zur Verfügung stünden. Schaut man bei diesem Aspekt zusätzlich auf die Gruppe der Geschäftsführer, zeigt sich: Die Hälfte nutzt keine Awareness Trainings aufgrund von fehlendem Budget. Dadurch wird deutlich, dass Firmenleiter oft das letzte Wort bei Investitionen und Anschaffungen im IT- und IT-Security-Bereich haben und vom Sinn und Nutzen von Maßnahmen für die Cybersicherheit überzeugt sein müssen, um diese mitzutragen.

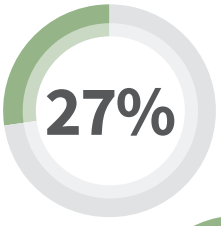
Die nötigen Gelder sind oft vorhanden, trotzdem werden sie den IT-Verantwortlichen nicht zur Verfügung gestellt, weil IT-Sicherheit keinen Return on Investment (ROI) generieren würde. Dabei refinanziert sich eine Maßnahme, sobald auch nur ein Cyberangriff dadurch erfolgreich abgewehrt wurde. Deutlich wird hier die Notwendigkeit, in der Verplanung des Budgets umzudenken. Für notwendige IT-Sicherheitsmaßnahmen müssen die finanziellen Mittel im ausreichenden Maße zur Verfügung stehen. Für die Geschäftsführung muss IT-Security daher einen höheren Stellenwert erhalten.

SECURITY AWARENESS FÜR MEHR IT-SICHERHEIT UND COMPLIANCE

Die Verbesserung der IT-Sicherheit als Ziel von Security Awareness Trainings liegt auf der Hand, es zeigen sich bei dieser Umfrage aber zwei Lager: Kommt der Befragte aus dem technischen Umfeld, ist die Verbesserung der IT-Sicherheit der Hauptgrund – dieses ist für die Hälfte der Mittelständler entscheidend. Teilnehmer aus dem Bereich Human Resources zielen mit den Schulungsmaßnahmen insbesondere auf die Einhaltung von Gesetzen und Regularien. Generell strebt mehr als ein Viertel (27 Prozent) mit Hilfe der Schulungen nach Compliance-Konformität. So übt die EU-Datenschutzgrundverordnung Druck auf die Verantwortlichen aus, das Unternehmen optimal und umfassend vor Cyberbedrohungen zu schützen.

„Unternehmen haften im Rahmen der angedrohten Bußgelder [der EU-Datenschutzgrundverordnung] für schuldhafte Datenschutzverstöße“, erklärt Stefan Sander, Rechtsanwalt und Fachanwalt für IT-Recht. „Solche Weiterbildungsmaßnahmen sind zwingender Bestandteil der organisatorischen Maßnahmen, die jeder Verantwortliche zum Erreichen von Compliance zu ergreifen hat.“

Das Einbeziehen der Mitarbeiter sorgt dafür, dass diese regelkonform agieren können und teure Strafzahlungen für Verstöße vermieden werden.



streben mit Hilfe der Schulungen nach Compliance-Konformität

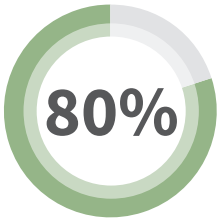
streben die Verbesserung der IT-Sicherheit an

DIE INVESTITION LOHNT SICH: AWARENESS TRAININGS VERBESSERN DIE IT-SICHERHEIT

IT-Security-Schulungen für Mitarbeiter lohnen sich für den Mittelstand: Fast neun von zehn Unternehmen (87 Prozent), die diese Maßnahme durchführen, erzielen positive Effekte. Das Budget ist damit gut angelegt und ein Return on Investment klar erreichbar.
Die überwiegende Mehrheit der Befragten beobachtet bei seinen Angestellten als Folge der Maßnahme einen viel vorsichtigeren Umgang mit dem Computer und den IT-Systemen. Dieses Fazit ziehen insbesondere 83 Prozent der teilnehmenden Geschäftsführer. Noch höher ist der Wert bei Unternehmen mit einem Jahresumsatz von mehr als 100 Millionen Euro: Für 88 Prozent zeigt sich eine positive Wirkung. Fast jede zweite mittelständische Firma (45 Prozent) stellt zudem fest, dass sie durch die Security Awareness Trainings weniger anfällig für Cyberangriffe sind. Das Ergebnis zeigt, dass die Mitarbeiter ihren entscheidenden Teil zur Cyberabwehr beigetragen und richtig gehandelt haben.

WIEDERHOLUNG VON INHALTEN IST TRUMPF BEI MITARBEITERSCHULUNGEN

Fast acht von zehn Unternehmen (80 Prozent) setzen auf Wiederholungen der Inhalte und dabei zeigt sich: Je grösser die Belegschaft ist, desto eher werden Security Awareness Trainings wiederholt. Das ist von entscheidender Bedeutung, denn Schulungsmaßnahmen für die Mitarbeiter müssen regelmäßig stattfinden und Inhalte wiederholt werden, um sie zu festigen. Dadurch bleiben die positiven Effekte der Security Awareness Trainings auf Dauer erhalten.



setzen auf Wiederholungen der Inhalte

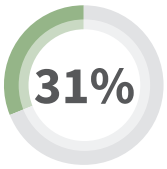
„Einmalige Trainingseinheiten, wie etwa Standalone-Web-based-Trainings für ein dediziertes Thema, haben zwar nach wie vor eine Daseinsberechtigung, sie sind aber in dieser Form nicht mehr nachhaltig genug. Gute Trainings sind so flexibel wie deren Lerner selbst. Moderne Lerntechnologien, vor allem in Form von modernen Learning-Management-Systemen und in Form sehr performanter E-Learning-Autorentools, schaffen es, dass Wissen modern und vor allem sehr flexibel vermittelt werden kann. Ein gutes Training wird in diesem Kontext im Optimalfall auch nach dessen Abschluss im Arbeitsalltag zur partiellen Wissensvermittlung weiterhin genutzt. So wird Theorie greifbar gemacht und Wissen wird nachhaltig gefestigt“, erklärt Christian Laber, E-Learning-Experte und Psychologe.

Der Blick auf die Jahresumsätze zeigt: Zwei Drittel (67 Prozent) der Unternehmen mit Einnahmen von weniger als einer halben Millionen Euro machen nur einmalige Schulungen für ihre Mitarbeiter. Das zur Verfügung stehende IT-Budget reicht in diesen Fällen nicht aus, um regelmäßige und nachhaltige Trainingsmaßnahmen zu finanzieren. Dabei dürfte sich der finanzielle Aufwand für einzelne Schulungen nicht rechnen, denn der Awareness-Grad der Mitarbeiter schrumpft kurze Zeit danach wieder auf das alte Niveau. Die Vergessenskurve des deutschen Psychologen Hermann Ebbinghaus zeigt, dass Gelerntes schnell wieder in Vergessenheit gerät. Nur durch kontinuierliche Wiederholungen steuern IT-Verantwortliche diesem Trend entgegen und sorgen dafür, dass sich das Wissen festigt. E-Learning-Angebote haben zudem den Vorteil, dass Sie deutlich günstiger in der Wiederholung sind als Präsenzunterricht.

NUR BEI DER HÄLFTE DER MITTELSTÄNDLER LERNEN ALLE MITARBEITER

Grundsätzlich ist IT-Sicherheit für alle Mitarbeiter ein wichtiges Thema, denn jeder kann ein Türöffner für eine Cyberattacke sein. Trotzdem verfolgen nur 56 Prozent der Mittelständler die Strategie, Security-Schulungen für die gesamte Belegschaft anzubieten, unabhängig von der Anzahl der Angestellten im Unternehmen oder der Position des Umfrageteilnehmers. Diese Unternehmen gehen das Thema Security Awareness ganzheitlich an. Oft haben viel mehr Mitarbeiter als gedacht Kontakt zu Kunden, arbeiten mit personenbezogenen oder vertraulichen Daten oder treffen sicherheitsrelevante Entscheidungen.

Die Hälfte der Mittelständler (53 Prozent) mit Einkünften von 500.000 bis fünf Millionen Euro spielen Security Awareness Trainings nur an ausgewählte Mitarbeiter aus. Generell berücksichtigen etwas weniger als ein Drittel (31 Prozent) einen ausgewählten Kreis von Angestellten bei den Schulungsmaßnahmen. Schulungen als Maßnahme für mehr Sicherheit können nur die volle Wirksamkeit entfalten, wenn alle Personen im Unternehmen dabei berücksichtigt werden und dafür muss das nötige Budget zur Verfügung stehen.



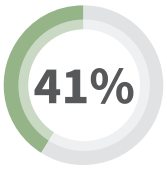
berücksichtigen einen ausgewählten Kreis von Angestellten bei den Schulungsmaßnahmen

Wie wichtig eine breite Schulung ist, zeigt die Betrugsmasche des CEO-Fraud. Hier werden oft gezielt Mitarbeiterinnen und Mitarbeiter aus der Buchhaltung angeschrieben, um fingierte Rechnungen zu bezahlen und die Rechnungssumme zu überweisen. Das macht deutlich: Eine Schulung etwa nur von Führungskräften ist nicht sehr sinnvoll.

PRÄSENZVERANSTALTUNGEN BEI SECURITY-SCHULUNGEN BEVORZUGT

Fast sechs von zehn Unternehmen (58 Prozent) setzen bei der Steigerung der Security Awareness auf Seminare oder andere Veranstaltungsformen, bei denen die Teilnehmer anwesend sein müssen. Insbesondere Geschäftsführer bevorzugen diese Art der Schulung: Fast drei Viertel der Firmenchefs (74 Prozent) setzen darauf. Mittelständler ab einem Jahresumsatz von fünf Millionen Euro setzen ebenfalls mehrheitlich auf die Präsenzveranstaltung.
Die zweitwichtigste Art im Mittelstand, Wissen rund um IT-Sicherheit zu vermitteln und zu teilen, ist der Versand von E-Mails oder die Bereitstellung der Informationen im firmeneigenen Intranet. Dies ist sinnvoll, aber nur als eine Ergänzung, um Mitarbeiter beispielsweise kurzfristig auf aktuelle Phishing-Kampagnen oder andere wichtige Themen aufmerksam zu machen. Ein IT-Security-Grundwissen lässt sich so bei Mitarbeitern nicht aufbauen, ein nachhaltiger Effekt kommt nicht zustande. Bei den Unternehmen mit Umsätzen bis fünf Millionen Euro ist dies allerdings die am häufigsten genutzte Form der Informationsvermittlung. Die eigene IT-Sicherheit steht nicht an erster Stelle. Diese Maßnahme ist kostengünstig, ersetzt aber keine ganzheitliche Trainingsmaßnahme.

Nur vier von zehn Mittelständler (41 Prozent) setzen auf fortschrittliche E-Learning-Angebote, obwohl diese einen viel nachhaltigeren Lernerfolg ermöglichen. Unternehmen mit einer größeren Belegschaft setzen eher auf diese moderne Unterrichtsform, als Firmen mit wenigen Mitarbeitern.



der Mittelständler setzen auf fortschrittliche E-Learning-Angebote

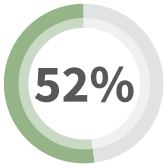
Security Awareness Trainings auf der Basis von E-Learning ist daher nachhaltiger und eine sinnvolle Investition für Unternehmen. 35 Prozent der befragten Unternehmen setzen zudem eine Phishing-Simulation ein, um Angestellte gezielt im Erkennen und Umgang mit Phishing- Mails zu schulen. Bei den Mittelständlern mit 501 bis 1.000 Mitarbeitern nutzen sogar die Hälfte diese zusätzliche Schulungsform. Phishing-Mails sind oft trickreich gestaltet, sodass es den Empfängern sehr schwerfällt, die gefährlichen Nachrichten zu enttarnen. Dadurch ist eine Phishing-Simulation eine sinnvolle Ergänzung eines IT- Security- Trainings. Zudem können IT-Verantwortliche auch hier messen, wie hoch der Awareness-Grad in der Belegschaft ist.

DIE VORTEILE VON E-LEARNING AUF EINEN BLICK

- Die Trainingseinheiten sind kurz und lassen sich leicht in den Arbeitsalltag integrieren. Das Wissen wird kleinteiliger und intensiver vermittelt, als es beispielsweise bei einem Tagesseminar der Fall ist.
- Trainingseinheiten können jederzeit von allen Mitarbeitern und von jedem Ort aus absolviert werden.
- Angestellte können sich weiterhin um das Kerngeschäft und ihre eigentlichen Aufgaben kümmern.
- E-Learning ist nach den neuesten didaktischen Methoden gestaltet und bindet unterschiedliche Medien in die Vermittlung des Wissens ein, zum Beispiel Videos.
- Der Wissensfortschritt ist für die IT-Verantwortlichen messbar.

PHISHING-SIMULATION SOLL EIN TEIL VON SECURITY AWARENESS TRAININGS SEIN

E-Learning ist eine sinnvolle Lernform für die Schaffung von Security Awareness. Der deutsche Mittelstand hat Erwartungen und Anforderungen an eine E-Learning-Dienstleistung: Die Hälfte (52 Prozent) möchte eine Phishing-Simulation bei den Mitarbeitern durchführen können. Dies ist besonders bei den Firmen mit mehr als 250 Angestellten der Fall. Bei den IT-Leitern, IT-Security-Beauftragten und CISOs (64 Prozent) haben etwa zwei Drittel diese Erwartungshaltung. Wichtig ist für 48 Prozent der Mittelständler aber auch die Berücksichtigung aktueller Cybercrime-Kampagnen und IT-Security-Themen, damit die Mitarbeiter auch immer auf dem neuesten Stand sind. Im gleichen Maße elementar für die Umfrageteilnehmer ist eine Reporting-Funktion. So können Verantwortliche den Lernfortschritt der Mitarbeiter nachvollziehen und dokumentieren – unter Einhaltung des geltenden Datenschutzes. Damit weist das mittelständische Unternehmen auch nach, dass es alle Maßnahmen ergreift, um Compliance-Konformität zu gewährleisten.



wollen bei den Awareness Trainings auch eine Phishing Simulation durchführen können

SICHERHEITSVORFÄLLE ALS WICHTIGSTES THEMA BEI IT-SECURITY-SCHULUNGEN

Bei Security Awareness Trainings ist für den deutschen Mittelstand das Thema Sicherheitsvorfälle, zum Beispiel der Befall des Netzwerkes mit einem Schadprogramm, am wichtigsten. Entscheidend ist oft die Art und die Geschwindigkeit, mit der Mitarbeiter auf Sicherheitsvorfälle reagieren, sofern sie diese überhaupt bemerken. Daher haben Unternehmen ein großes Interesse an dieser Thematik. Datenschutz und DSGVO-Compliance sind das zweitwichtigste Themenfeld, weil es neben der Sicherstellung der Wirksamkeit der Cyberabwehr die Regularien eine große Rolle spielen. Bereits die Fragestellung nach der Zielsetzung der Security Awareness Trainings ergab, dass viele Mittelständler Compliance-Konformität als Hauptgrund für die Durchführung von Security Awareness Trainings angeben. Phishing steht für Unternehmen auf Platz drei der wichtigsten Themen. Viele Mittelständler haben ein großes Interesse an einer Phishing-Simulation, um Mitarbeiter gezielt zu trainieren, weil E-Mails das Einfallstor Nummer eins bei Cyberangriffen auf Unternehmen sind.

FAZIT: DER MITTELSTAND STEHT SICH BEIM THEMA SECURITY AWARENESS SELBST IM WEG

Die meisten mittelständischen Unternehmen in Deutschland setzen auf Security Awareness Trainings. Dabei zeigen die Schulungsmaßnahmen eindeutig ihre Wirksamkeit: Sie steigern die IT-Sicherheit, lassen Mitarbeiter vorsichtiger mit IT-Ressourcen umgehen und sorgen zudem für Compliance-Konformität.

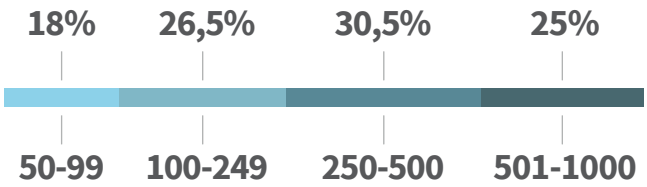
Allerdings nutzt nicht jeder Mittelständler das Potenzial der Mitarbeiter als Teil der Cyberabwehr. Eine Minderheit setzt auf eine rein technisch basierte IT-Sicherheits-Infrastruktur und glaubt, dass sie damit gut aufgestellt ist. Dabei führen die Hälfte der befragten Unternehmen ein Security-Vorfall in Vergangenheit auf das fehlerhafte Verhalten eines einzelnen Mitarbeiters zurück. Ein weiteres Problem: Einige Firmen führen nur einmalige Schulungen durch, die nicht nachhaltig sind und deren Effekt rasch verpufft. Zudem beziehen IT-Verantwortliche im Mittelstand oft nicht alle Mitarbeiter bei den Security- Awareness-Schulungen mit ein und setzen konservativ auf Präsenzveranstaltungen, anstatt auf zielführende E-Learnings. Dabei bietet diese Lernform deutliche Vorteile.

Die Umfrage zeigt zudem deutlich, dass IT-Sicherheit stark vom Budget abhängig ist. In einigen Unternehmen, insbesondere bei kleineren Mittelständlern, scheinen die notwendigen Gelder für einen umfassen Schutz nicht zur Verfügung zu stehen, weil sie falsch priorisiert und verteilt werden. IT-Sicherheit scheint immer noch nicht den nötigen hohen Stellenwert zu haben, um in eine umfangreiche IT-Security-Architektur zu investieren. Der deutsche Mittelstand verspielt hier leichtfertig seine eigene Sicherheit und im schlimmsten Fall auch seinen wirtschaftlichen Erfolg. Hier ist ein zeitnahes und radikales Umdenken von Nöten.

Security Awareness Trainings leisten einen wichtigen Beitrag zur umfassenden Cyberabwehr und sind eine perfekte Ergänzung für technische Maßnahmen, wie beispielsweise die Separierung von Netzwerken oder den Einsatz einer Sicherheitslösung. Diese Erkenntnis ist noch nicht überall im Mittelstand angekommen, dabei drängt die Zeit – denn: Jeder Tag ohne geschulte Mitarbeiter ist ein verlorener Tag für die IT-Sicherheit.

ÜBER DIE UMFRAGE

Für die Security Awareness Trainings Umfrage hat OmniQuest im Auftrag von G DATA CyberDefense AG im Herbst 2020 insgesamt 200 deutsche Unternehmen befragt, die dem Mittelstandssegment angehören. Die befragten Firmen hatten zwischen 50 und 1.000 Mitarbeiter. Die Branchenzugehörigkeit und das Tätigkeitsfeld spielten dabei keine Rolle.



Anzahl der Mitarbeiter in 200 Unternehmen

ÜBER G DATA CYBERDEFENSE

Mit umfassenden Cyber-Defense-Dienstleistungen macht der Erfinder des AntiVirus Unternehmen verteidigungsfähig gegen Cybercrime. Mehr als 500 Mitarbeiter sorgen für die digitale Sicherheit von Unternehmen und Anwendern. Forschung und Entwicklung erfolgen in Deutschland.

G DATA schützt mit NextGen-KI-Technologien, Endpoint Protection, bietet Penetrationstests und Incident Response bis zu Awareness-Trainings, um Unternehmen wirksam zu verteidigen.

G DATA Lösungen wurden vielfach ausgezeichnet, zuletzt mit einem Doppelsieg beim PUR-Award für Malwareschutz und E-Mail-Security.