Security Awareness Trainings als Umsatz-Booster

10 Gründe, warum ITK-Reseller Security Awareness Trainings im Portfolio haben sollten

www.kaspersky.de

#truecybersecurity

Einleitung

Die meisten Unternehmen wissen, dass sie sich heutzutage nicht ausschließlich auf eine gute Endpoint-Security-Software verlassen können. Zudem fordern neue gesetzliche Rahmenbedingungen wie die Datenschutzgrundverordnung zusätzliche Absicherungen der IT-Systeme und mehr Verständnis für Datenschutz. Ohne ein passendes Portfolio mit den notwendigen Tools ist es jedoch schwierig und zeitaufwendig, diese Vorgaben einzuhalten.

Für Partner, die im ITK-Vertrieb tätig sind, bringt dies neue Herausforderungen an ihr Lösungsangebot mit sich, bietet aber gleichzeitig fantastische Möglichkeiten, um sich bei Unternehmen nicht nur als Softwarelieferant, sondern auch als Sicherheitsberater und Auditor zu positionieren. In diesem Whitepaper liefern wir Ihnen deshalb 10 Gründe, warum Sie Security Awareness Trainings in Ihr Portfolio aufnehmen sollten.

Dies sind einige der Herausforderungen, denen Sie wahrscheinlich gegenüberstehen:

Gestiegene Sicherheitsanforderungen und neue Gesetzesvorgaben

Nicht nur Unternehmen machen die wachsenden Anforderungen an IT-Sicherheit zu schaffen, auch Reseller sehen sich damit konfrontiert und es sind häufig viele Fragen offen. Vor allem die Umsetzung der DSGVO fühlt sich oft an wie das berühmte Fass ohne Boden. Wie können Sie ein solches Thema einfach angehen und darüber hinaus Ihre Kunden professionell beraten?

Der Markt bietet viele Lösungen für jeden Bedarf – aber welche brauche ich für meine Kunden?

Oft versuchen sich die Hersteller mit innovativen Sicherheitslösungen gegenseitig zu übertreffen. Doch wie finden Sie die Lösung, die wirklich für Sie als Reseller und Ihre Kunden die beste Variante ist? Durch die Vielfalt steigt das Risiko, den Überblick zu verlieren und das Wichtige zu übersehen.

Hoher Schulungsaufwand vorab – gerechtfertigt?

Hat man eine Lösung gefunden, geht die Rechnerei los. Wie hoch ist der Schulungsbedarf für Sie als Reseller und können Sie die Zeit dafür aufbringen? Was erwarten Sie an Resultaten und rechtfertigen diese Ihr eigenes unternehmerisches Risiko? Bietet der Hersteller Programme und Support an, worauf Sie zurückgreifen können?

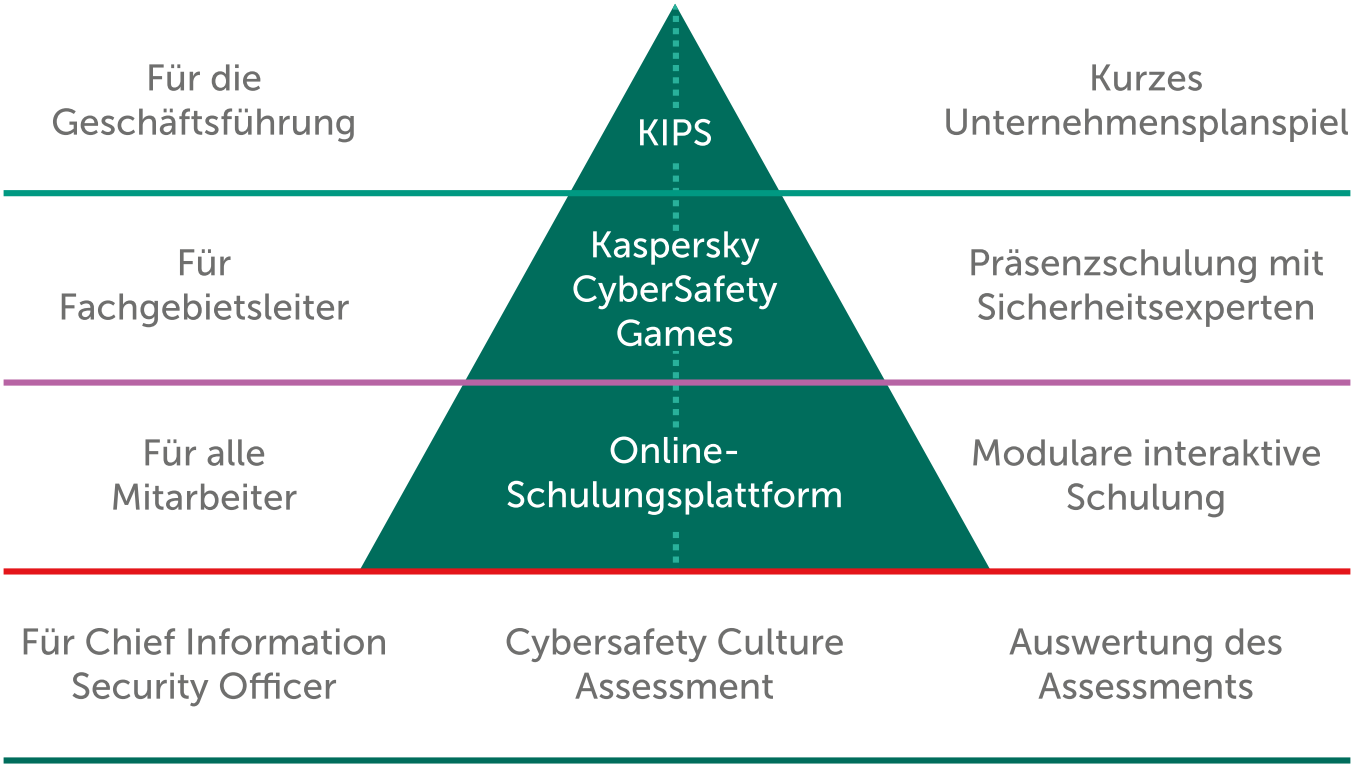
Lizenzierungsprogramme zum Verzweifeln

Häufig gleichen Lizenzprogramme einer Doktorarbeit. Sich da zurechtzufinden, ist oft wie das Suchen der Nadel im Heuhaufen. Als Partner haben Sie aber keine Zeit, sich mit komplizierten Abrechnungen zu beschäftigen, schon gar nicht, wenn Ihr Portfolio mehrere Hersteller umfasst.

Einer Umfrage[1] von Kaspersky Lab und B2B International zufolge sehen 52 % der Unternehmen in ihren Mitarbeitern das größte Risiko für ihre IT-Sicherheit, da sie die IT-Sicherheitsstrategie durch fahrlässiges Handeln oder mangelnde Kenntnisse gefährden.

Unternehmen befürchten vor allem, dass Mitarbeiter unangemessene Daten über ihre mobilen Geräte weitergeben (47 %), durch den physischen Verlust mobiler Geräte das Unternehmen Risiken aussetzen (46 %) sowie IT-Ressourcen unsachgemäß nutzen (44 %).

[1] Der menschliche Faktor in der IT-Sicherheit: Wenn Mitarbeiter zum Risikofaktor werden – Juni 2017



Das Schulungsportfolio von Kaspersky Lab für Mitarbeiter in Unternehmen bietet für jeden Bereich im Unternehmen ein dediziertes Training

Bei näherer Betrachtung dieser Ergebnisse variieren diese Bedenken hinsichtlich einer unsachgemäßen Nutzung von IT-Ressourcen durch Mitarbeiter je nach Unternehmensgröße erheblich: Sehr kleine Unternehmen (1 bis 49 Mitarbeiter) fühlen sich durch diesen Punkt stärker bedroht als Unternehmen mit mehr als 1000 Mitarbeitern. Dies könnte mit verschiedenen Faktoren zusammenhängen, etwa, dass Großunternehmen striktere Richtlinien definieren

Ich bin überzeugt, aber wie überzeuge ich nun meine Kunden?
Im Idealfall zeigen Ihnen die Hersteller auf, wo aus Kundensicht die Probleme liegen, die Sie als Reseller lösen können. Über was sollte Ihr Kunde jetzt nachdenken? Wer ist von bestimmten Cyberbedrohungen betroffen und warum? Mit wem im Unternehmen sollten Sie überhaupt über Security-Lösungen sprechen? Ist Ihr Kunde erst einmal überzeugt, muss alles reibungslos laufen. Dazu sollte klar sein, wie der Einkaufs- und Bestellprozess für Sie aussieht und auf wen Sie im Fragefall zurückgreifen können.

Wir haben jetzt schon so viel zu tun – wie soll ich künftig noch mehr Ressourcen bereitstellen?

Klar, mehr Umsatz ist immer gut. Aber steht er im Verhältnis zum Aufwand? Je einfacher Kunden zu überzeugen sind, desto leichter ist die Abwicklung Ihres Geschäfts. Und je geringer der After-Sales-Aufwand, desto höher der Gewinn. Sie sollten sich daher auf Projekte konzentrieren, die einen hohen Deckungsbeitrag liefern und gleichzeitig stark nachgefragt werden. Zudem sollten Sie immer auf Ihren Distributionspartner zurückgreifen können, der Sie als externe Fachabteilung bei der Geschäftsgenerierung unterstützt. Dies kann unter anderem durch Marketingmaßnahmen, Dienstleistungen, Budgets, Terminsupport bei Kundenmeetings oder auch geführte Kundenveranstaltungen geschehen.

Endpoint-Sicherheit – habe ich schon

Glücklicherweise sind mittlerweile die meisten Unternehmen mit einer AV-Software ausgestattet. Doch der Bedarf hat sich verändert. Unternehmen brauchen umfassendere Sicherheitskonzepte. Will man dieser Tatsache entgegenkommen, findet man sich oft im direkten Wettbewerb zu anderen Security-Anbietern. Es gibt jedoch viele Möglichkeiten, um mit neuen Kunden ins Gespräch zu kommen und das ganz unabhängig von Endpoint-Sicherheit.

1. Grund: Der Mitarbeiter ist das Risiko

[1] IBM 2015 Cyber Security Intelligence Index, Information Security Breaches Survey 2015. HM Government in Zusammenarbeit mit InfoSecurity Europe und PwC.

[2] https://www.kaspersky.de/about/press-releases/2017_vulnerability-46-percent-of-cyber-security-incidents-can-be-attributed-to-the-misconduct-of-employees

Noch vor einigen Jahren entstanden über **80 %** aller Cybersicherheitsvorfälle durch menschliche Fehler.[1] Auch wenn eine jüngere Studie von Kaspersky Lab mit einem Wert von **46 %** eine Verbesserung der Situation belegt, zeigt sie zugleich, dass bei ca. **40 %** der weltweit befragten Unternehmen die Mitarbeiter versuchen, selbst verschuldete Cybersicherheitsvorfälle aus Angst vor Konsequenzen geheim zu halten.[2] Ein gravierendes Problem: Unternehmen verlieren Millionen bei der Wiederherstellung von Vorfällen, die durch Mitarbeiter verursacht wurden. Die Folgekosten sind vor allem aufgrund der neuen DSGVO-Gesetzeslage enorm hoch. Unternehmen haben daher ein großes Interesse daran, dieses Risiko auf ein Minimum zu reduzieren.

Klassische Schulungsprogramme bzw. Vor-Ort-Weiterbildungen können Mitarbeitern die erforderlichen Verhaltensänderungen und die nötige Motivation für mehr Security-Bewusstsein häufig nicht vermitteln. Wenn überhaupt, haben solche Trainings nur einen kurzfristigen Effekt, und sie sind im Vergleich zu Online-Schulungen recht teuer.

Eine deutlich langfristigere Wirkung haben computerbasierte Trainings, die individuell auf Mitarbeiter zugeschnitten sind und anschaulich Wissen vermitteln. Unternehmen profitieren davon, dass sie mit Online-Schulungen das Know-how auch messbar machen können. Dies steigert nicht nur generell die positive Haltung gegenüber dem Thema IT-Sicherheit im Unternehmen, sondern ermöglicht es, IT Security abteilungsübergreifend fest in den Köpfen der Mitarbeiter zu verankern.

2. Grund: Der Markt ist riesig

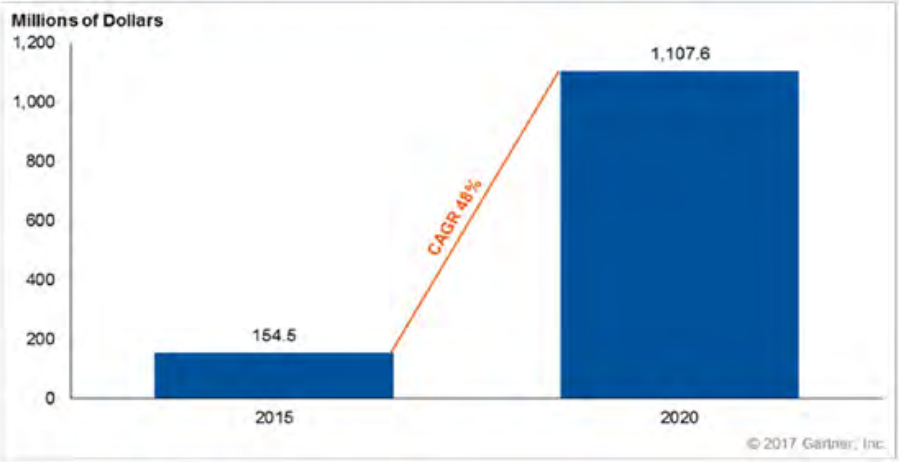
Der Investitionsmarkt für computerbasierte Awareness Trainings wird laut Gartner (2017) von **2015 bis 2020** um mehr als **700 %** auf rund 1,1 Mrd. US-Dollar steigen. Hier können Sie stark von einem Aufschwung in der Nachfrage ausgehen und sich bereits jetzt dafür rüsten.

Einer aktuellen Studie zufolge geben lediglich **3 %** der Unternehmen an, dass Endpoint-Lösungen als Hürde beim Schutz vor Cyberbedrohungen im Unternehmen relevant sind. Sie haben vielmehr erkannt, dass der Mitarbeiter selbst eine entscheidende Rolle spielt. Denn fast **50 %** der Unternehmen sehen eines der größten Risiken für die Cybersicherheit bei nicht oder schlecht ausgebildeten Mitarbeitern bzw. nicht verfügbaren Trainings. Fehlendes Budget bleibt jedoch an erster Stelle.

https://www.gartner.com/newsroom/id/3836563

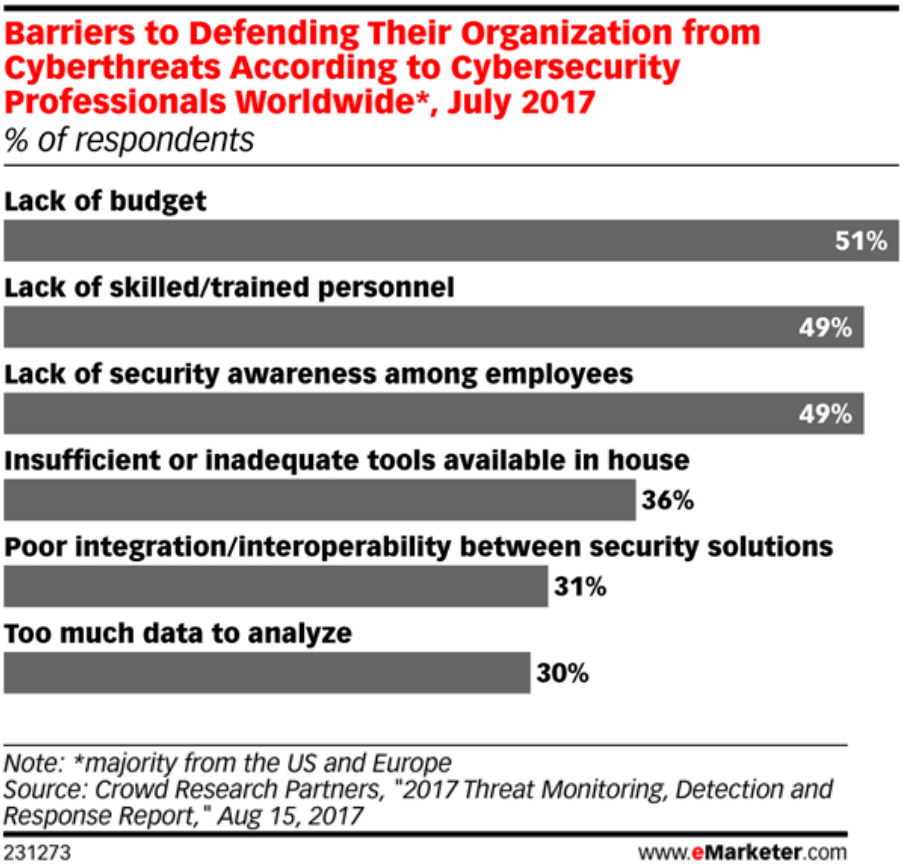
Market Size and Compound Annual Growth Rate

Figure 1. Spending on Security Awareness Computer-Based Training, Worldwide, 2015 and 2020



CAGR = compound annual growth rate

Source: Gartner (March 2017)



Kaspersky Lab hat deshalb eine Reihe von computergestützten Schulungsprodukten auf den Markt gebracht, die auf den neuesten Lerntechniken basieren und an sämtliche Unternehmensebenen gerichtet sind.

3. Grund: Rechtlich ist jedes Unternehmen zu Security-Maßnahmen verpflichtet

[3] https://dsgvo-gesetz.de/themen/privacy-by-design/

Spätestens seit der Einführung der DSGVO ist jedes Unternehmen zu Privacy by Design (Schutz durch das Unternehmen selbst) verpflichtet. Dazu gehört in erster Linie, die Mitarbeiter darüber zu informieren, wie sie mit Daten umgehen sollten und wie sich das Risiko des Datenverlustes vermeiden bzw. ausschließen lässt. Dies können Unternehmen mittels einer einmaligen Vor-Ort-Schulung machen, bei der sie sich am Ende die Teilnahme der Mitarbeiter durch Unterschriften bestätigen lassen – oder sie wählen eine Schulungsplattform im Rahmen eines nachhaltigen und für Mitarbeiter erlebbaren Security-Awareness-Konzepts. Auch damit hat das Unternehmen nachweislich und transparent die Anforderungen erfüllt und kann Mitarbeiter kontinuierlich zum Datenschutz animieren.

Durchschnittliche finanzielle Folgen des Fehlverhaltens von unachtsamen/ unwissenden Mitarbeitern[1]

Für kleine/mittlere Unternehmen
- Unangemessene Weitergabe von Daten – 88 000 $
- Verlust von Mobilgeräten, durch die Unternehmen Risiken ausgesetzt werden – 99 000 $
- Verlust von Geräten oder Medien, die Daten enthalten – 81 000 $
- Unsachgemäße Nutzung von IT-Ressourcen durch Mitarbeiter – 68 000 $

Für Großunternehmen
- Vorfälle mit „non-computing", angeschlossenen Geräten – 1,6 Mio. $
- Verlust von Geräten oder Medien, die Daten enthalten – 1,1 Mio. $
- Unsachgemäße Nutzung von IT-Ressourcen durch Mitarbeiter – 581 000 $
- Unangemessene Freigabe von Daten über Mobilgeräte – 464 000 $

Datenschutzverletzungen in Zahlen[2]:
- 61 % der Opfer von Datenschutzverletzungen im Jahr 2017 waren Unternehmen mit unter 1000 Mitarbeitern
- 81 % der Hacker machten sich für einen Angriff gestohlene Passwörter und/ oder schwache oder leicht zu erratende Passwörter zunutze
- 43 % der Datenschutzverletzungen erfolgten über soziale Netzwerke
- 66 % der Malware wurde über schädliche E-Mail-Anhänge installiert

[1] „Global IT Security Risks Survey 2017". Kaspersky Lab und B2B International
[2] „2017 Data Breach Investigations Report" Verizon

4. Grund: Budgetknappheit – weniger relevant

Die Investitionsbereitschaft von Unternehmen in IT-Sicherheit ist Studien zufolge immens groß, doch oft hört man, wie knapp die Budgets vor allem bei kleinen und mittelständischen Unternehmen sind. Bei IT-Sicherheitsschulungen sprechen wir allerdings von der Ausbildung der eigenen Mitarbeiter. Das Interesse der IT-Abteilung hierfür ist sehr groß, aber noch größer ist vermutlich der Zuspruch der Personalabteilung und des Datenschutzbeauftragten. Und genau dort werden Budgets für Schulungen bereitgestellt. Sie sollten also im Erstgespräch mit Ihrem Kunden kommunizieren, dass das erforderliche Budget aus der Personalabteilung kommen wird, was wiederum die IT-Abteilung entlastet.

In dieser Grafik zeigen wir Ihnen auf, welche Unternehmensbereiche beim Thema Security Awareness involviert sind und bei entsprechenden Maßnahmen auch beteiligt werden müssen:

5. Grund: Ein idealer Türöffner

Allein über den Ansatz „Endpoint Security" werden Sie Schwierigkeiten haben, mit wenig Aufwand erfolgreich zu sein. Denn wie bereits erläutert, haben viele Unternehmen bereits eine entsprechende Lösung. Hier können Sie meist nur dann ein Geschäft abschließen, wenn der Preis Ihres Produktes unschlagbar ist und die bisher eingesetzte Lösung nicht zufriedenstellend läuft. Beim Thema Security Awareness Trainings rennen Sie jedoch sprichwörtlich offene Türen ein. Weltweit sehen 50 % der Unternehmen die Umsetzung als schwierig an, dennoch beschäftigt sich aufgrund der DSGVO aktuell fast jedes Unternehmen mit Schulungskonzepten zum Aufbau von Sicherheitsbewusstsein.

Sie können mit der Kaspersky-Plattform für Security Awareness eine Lösung vorschlagen, die einfach zu administrieren ist, das IT-Budget nicht belastet und für alle Abteilungen einen echten Mehrwert bietet. Die Erfolgsaussichten sind enorm. Und haben Sie diesen ersten Schritt getan, gibt es weitere Möglichkeiten für Neugeschäfte.

6. Grund: Riesiges Cross- und Upselling-Potenzial

Haben Sie ein Unternehmen überzeugt und als Kunden gewonnen, können Sie auch Ihr komplettes Portfolio besser platzieren, denn nun kennen Sie den Bedarf, die IT-Architektur und die Investitionsbereitschaft Ihres Neukunden. Ist er zufrieden, wird er sich gerne über weitere Leistungen von Ihnen informieren. Vielleicht werden Sie dadurch sogar zum neuen Hardware-Lieferanten oder Anbieter von zusätzlichen Softwarelösungen. Mit Services runden Sie Ihr Angebot ab, zum Beispiel lassen sich fixe Quartalsmeetings vereinbaren, in denen die Resultate der Schulungen besprochen werden und Sie das nächste Quartal planen.

7. Grund: Kunden wollen keinen Händler – sie wollen einen Berater

IT-Sicherheit ist komplex. Vor allem kleinen und mittelständischen Unternehmen mangelt es hier an Know-how und Ressourcen. Sie können sich deshalb bei Ihren Kunden nicht nur als Händler, sondern auch als Sicherheitsberater positionieren. Denn das Problem der IT-Komplexität können Sie lösen, indem Sie diese jedem Mitarbeiter verständlich machen. Mit den Security Awareness Trainings von Kaspersky Lab können Sie ein komplettes Schulungskonzept passgenau für die einzelnen Abteilungen Ihres Kunden entwickeln, konfigurieren und ausrollen – in mehreren Sprachen und mit zeitgesteuerten Trainingsplänen. Damit bieten Sie einen Service an, der honoriert wird und Ihr Geschäft vorantreibt.

Jeder Kunde hat sicherlich andere Anforderungen, aber dennoch können Kaspersky-Partner ein gewisses Grundkonzept verfolgen, das – wenn es einmal erstellt ist – gewissermaßen auf andere Kunden übertragen werden kann. Bei der Entwicklung stehen Ihnen sowohl unsere Distributionspartner als auch die Experten von Kaspersky Lab gerne zur Verfügung.

8. Grund: Kurzer Sales Cycle

Bei den meisten Softwareprojekten geht man von einem minimalen Verkaufszyklus von sechs, meist aber eher zwölf Monaten aus. Mit der Kaspersky Security Awareness Plattform können Sie ein Kundenprojekt im Regelfall schon innerhalb der ersten drei Monate fakturieren. Die Implementierungszeit ist extrem kurz, der Aufwand überschaubar und die Verfügbarkeit der Lösung immer gewährleistet. Zudem ist das Lizenzierungsmodell äußerst einfach, da per Mitarbeiter lizenziert wird.

In den kommenden Monaten werden wir von Kaspersky Lab den Service weiter ausbauen und neben der klassischen Lizenzierung auch eine weitere Lizenzierungsform anbieten, bei der vor allem Managed Service Provider die Lösung über ein flexibles und skalierbares Modell an ihre Kunden weitergeben können.

9. Grund: Kosten

Vergleicht man die Investitionen in klassische Schulungen, bei denen ein Trainer zum Beispiel einen Vortrag zur Datensicherheit hält, mit den Kosten der Security Awareness Plattform, stellt man schnell fest, wie viel günstiger ein Unternehmen Weiterbildungen für Mitarbeiter durchführen kann. Eine physische Schulung schlägt im SMB-Umfeld mit mindestens ein paar tausend Euro zu Buche, der Effekt ist jedoch meist weder nachhaltig noch messbar. Denn stellen Sie sich vor, wie gern Sie selbst in einem Meeting-Raum sitzen würden, um einen ganzen Tag eine Schulung zu einem für Sie trockenen Thema zu absolvieren.

Mit der Security Awareness Plattform erhalten Ihre Kunden über 30 verschiedene Trainingsmodule. Mitarbeiter können ein ganzes Jahr die komplette Plattform nutzen. Zudem sind die Schulungen interaktiv: Das System zeigt praxisnahe Situationen aus dem Arbeitsalltag, in die der Mitarbeiter direkt einbezogen wird. Bei 100 Anwendern kostet die Plattform nicht mehr als zwei physische Schulungen pro Jahr. Neben den Trainingsmodulen haben Unternehmen zudem die Möglichkeit, anhand von simulierten Phishing-Angriffen, Assessments und Wissenstests mit vorgegebenen und kundenspezifischen Fragen den Wissensstand der Mitarbeiter zu ermitteln.

10. Grund: Bester Support und Einstieg

So ziemlich jedes Unternehmen legt in der heutigen Zeit Wert darauf, seine Mitarbeiter im Bereich Cybersicherheit zu schulen, und wird Ihnen dahingehend Gehör schenken. Egal ob es sich dabei um Unternehmen aus den Branchen Energie, Fertigung, Handel, Industrie und kritische Infrastrukturen handelt oder um Behörden, Finanzdienstleister und sonstige Organisationen, die besonders auf die Anforderungen der DSGVO eingehen müssen. Gerade für Personen, die Mitarbeitertrainings organisieren oder Verantwortung für die Ausbildung der Mitarbeiter haben, ist die Security Awareness Plattform interessant.

Fazit

Unternehmen verzweifeln zunehmend an der Komplexität moderner IT-Systeme. Sie müssen gleichzeitig einen reibungslosen Betrieb sicherstellen und Kosten sparen. Oberste Priorität hat dabei die IT-Sicherheit. Hierfür ist es wichtig, dass die Menschen im Unternehmen potenzielle Cyberbedrohungen frühzeitig erkennen und richtig darauf reagieren. Allerdings beklagen fast **50 %** der Unternehmen weltweit, dass Mitarbeiter schlecht geschult sind und erforderliche Trainings-Tools fehlen. Ein Sicherheitsrisiko, denn mehr als **46 %** aller Cybersicherheitsvorfälle gehen auf menschliche Fehler zurück. Unternehmen verlieren Millionen bei der Wiederherstellung von Vorfällen, die durch Mitarbeiter verursacht wurden. Klassische Schulungsprogramme oder Vor-Ort-Weiterbildungen können Mitarbeitern die nötige Motivation zur Verhaltensänderung häufig nicht vermitteln. Als ITK-Partner von Kaspersky Lab lösen Sie dieses Problem mit der Security Awareness Plattform.

Der Markt erfordert eine neue Ansprache, aber bietet Partnern auch enormes Potenzial, Kunden zu gewinnen, diese zu halten und auszubauen sowie gleichzeitig zu deren Sicherheitsberater zu werden. Mit einer sehr einfachen Lösung können Sie also bei Ihren Kunden sehr viel erreichen.

Starten Sie in diesen lukrativen Markt mit Kaspersky Lab. Wir freuen uns auf Sie!

Bis zu	Weniger als	Bis zu	Mehr als	Mehr als
90%	**50%**	**93%**	**30x**	**86%**
Reduzierung der IT-Sicherheits-vorfälle	Reduzierung der Kosten von IT-Sicherheits-vorfällen	Erfolgsquote das das Wissen im Alltag ange-wendet wird	ROI des Investments in Security Awareness	der Teilnehmer empfehlen Security Awareness Trainings weiter

Lösungsübersicht

Kaspersky Security Awareness Plattform

Kaspersky®
Cybersecurity
Awareness Training

Mehr Informationen:
https://www.kaspersky.de/enterprise-security/security-awareness

Plattform-Demo:
https://www.kaspersky.de/enterprise-security/cybersecurity-awareness/demo

Wollen Sie durchstarten?
Nehmen Sie hier Kontakt zu uns auf.

Die modulare Onlineschulungsplattform von Kaspersky Lab richtet sich an alle Mitarbeiter eines Unternehmens. In interaktiven Übungen und anhand typischer Szenarien des Arbeitsalltags lernen die Teilnehmer direkt an ihrem Computer mehr über potenzielle IT-Bedrohungen und den Umgang damit. Simulierte Phishing-Angriffe sowie spezielle Trainingsmodule beispielsweise zu sicherem Surfen, Passwort-Sicherheit und Datenschutz schulen die Mitarbeiter und sensibilisieren sie im Umgang mit möglichen Cyberbedrohungen. Steigern Sie mit Kaspersky Lab das Sicherheitsbewusstsein bei Ihren Kunden!

Fast Facts:

- **32 Lernmodule** mit 10–20 Minuten Bearbeitungszeit pro Modul
- **Module zu DSGVO, Ransomware, Passwort-Sicherheit, E-Mail-Sicherheit** etc.
- **Inklusive 35 Sprachen** (Deutsch, Englisch, Italienisch, Spanisch, ...)
- Ermittlung des eigenen Wissens durch **Wissenstests**
- **Simulierte Phishing-Angriffe** mit vielen veränderbaren Vorlagen
- **Umfangreiche Reporting- und Analyse-Funktion**
- Einfache, aber umfassende **Administrationsmöglichkeiten**

Kaspersky Lab

Cybersicherheit für Unternehmen:
www.kaspersky.de/enterprise
Neues über Cyberbedrohungen:
www.viruslist.de
IT-Sicherheitsnachrichten:
business.kaspersky.com

#truecybersecurity
#HuMachine

www.kaspersky.de