Bild: apiran/Fotolia.com

(K)ein Klick zu viel

Die überragende Mehrheit aller Cyberangriffe beginnt mit einer Person, die einen Fehler macht. Awareness-Trainings sollen dieser «Schwachstelle Mensch» entgegenwirken und vor den Bedrohungen in der Mailbox, im Web und in fremden USB-Sticks sensibilisieren. Was dabei essenziell ist, sagen Experten von Avantec, Axians, Digicomp, G Data, Infoguard, Ispin, Lucy Security und RedIT. Interviews: Coen Kaat

Markus Graf
COO, Avantec

Weshalb sind Security-Awareness-Trainings wichtig? Dass man nicht auf irgendwelche komischen Links klicken sollte, weiss man doch unterdessen.
Markus Graf: Security-Awareness-Trainings sind eine der wenigen Möglichkeiten, um das wichtigste Puzzleteil in der IT-Security mit ins Boot zu holen: die Mitarbeiterinnen und Mitarbeiter. Sie sind das Ziel unzähliger Angriffsversuche und gleichzeitig wichtige Sensoren in unserem Netzwerk. Die Angriffe beschränken sich längst nicht mehr auf Mails in schlechtem Deutsch und auffällige Links. Das Erkennen von Angriffen durch die Mitarbeitenden bedingt Wachsamkeit und Aufmerksamkeit. Mit Awareness-Trainings wird dies gezielt geschult und gefördert.

Was ist der Schlüssel zum Erfolg bei Awareness-Trainings?
Das Training muss auf den Kunden und seine Mitarbeitenden zugeschnitten werden. Nach gewissen Basisinformationen wird mittels Fragen und spielerischen Elementen die Security-Maturität jeder Mitarbeiterin und jedes Mitarbeiters bestimmt und darauf werden die Lerninhalte optimiert. Praxisnahe Beispiele aus dem Alltag schaffen die Brücke zwischen Theorie und Arbeitsalltag.

Was müssen Reseller selbst können/wissen, um derartige Trainings erfolgreich anzubieten?
Lernerfolge sind kontinuierlich zu beobachten und die Schlüsse daraus sind individuell in neue Kampagnen einzuarbeiten. Da ergibt es Sinn, die Umgebung zu kennen. Zudem ist die Absprache zwischen Kunde, Partner und Hersteller wichtig, damit die Erwartungen an die Trainings erfüllt werden können.

Inwiefern führt das Angebot von Awareness-Trainings zu weiterem Business für Reseller?
Das Anbieten von Awareness-Trainings erzeugt für einen Reseller nicht direkt weiteres Business. Ein auf Security sensibilisierter Kunde ist aber eher bereit, sich mit dem Thema IT-Security auseinanderzusetzen und sich konkret zu informieren. Darum ist es elementar, sich mit Kunden über ganzheitliche Security auszutauschen, bei der auch nicht-technische Aspekte eine Rolle spielen. Awareness-Trainings können dabei ein Element der Security-Strategie darstellen.

Alexander Reusch
Chief Sales Officer, Axians Cyber Security

Weshalb sind Security-Awareness-Trainings wichtig? Dass man nicht auf irgendwelche komischen Links klicken sollte, weiss man doch unterdessen.
Alexander Reusch: Die Realität sieht leider anders aus. Nach wie vor sind viele erfolgreiche Cyberattacken auf Phishing-Kampagnen zurückzuführen. Zu wenige Mitarbeitende sind sich der Risiken im Cyberspace tatsächlich bewusst und noch weniger sind in der Lage, Attacken zu erkennen. Dazu entwickeln sich Phishing-Attacken ständig weiter und werden immer raffinierter. Auch greifen Kriminelle bei ihren Ausspähversuchen auf Methoden der Angewandten Sozialwissenschaften (Social Hacking) zurück. Die Zielpersonen werden dabei psychologisch so bearbeitet, dass sie gar nicht anders als mit einem bestimmten, vom Angreifer gewünschten, Verhalten reagieren können. Hierzu werden sie ausspioniert, es werden ihnen falsche Informationen vorgespielt, sie werden so lange psychischem Druck ausgesetzt, bis sie endlich in der gewünschten Art und Weise reagieren.

Was ist der Schlüssel zum Erfolg bei Awareness-Trainings?
Wie bei allen Trainings basiert der Erfolg auf Kontinuität. Cyber Awareness darf kein einmaliges Ereignis sein und auch das klassische sich

jährlich wiederholende Cyber-Training hat ausgedient. Oft wird in Unternehmen Awareness-Training im Sinne einer Alibi-Übung durchgeführt, beziehungsweise um Compliance-Anforderungen zu erfüllen. Erfolgreiches Awareness-Training setzt auf eine Kombination aus kontinuierlichen Trainings-, Test- und Analyseeinheiten. Dies bedeutet, dass die Lernfortschritte der Mitarbeitenden durch gezielte Angriffssimulationen ständig überprüft und die Trainingsmodule dynamisch angepasst werden. Die Trainingsinhalte sollten dabei aktuell und vielseitig sein. Es gilt, die Mitarbeitenden zu motivieren, einen Teil der aktiven Cyberabwehr zu werden. Aus diesem Grund muss Training auch Spass machen.

Was müssen Reseller selbst können/wissen, um derartige Trainings erfolgreich anzubieten?
Awareness-Trainings müssen darauf ausgerichtet sein, das Sicherheits- und Risikobewusstsein der Mitarbeitenden schnell und nachhaltig anzuheben. Diese sollten auf einer praxisbewährten Kombination von Schulungseinheiten, Tests im Arbeitsalltag sowie qualitativen Analysen basieren. Dazu muss man als Partner die täglichen Herausforderungen des Unternehmens und deren Mitarbeitende verstehen.

Inwiefern führt das Angebot von Awareness-Trainings zu weiterem Business für Reseller?
Cybersecurity Awareness ist ein wichtiger Bestandteil der Sicherheitsstrategie von Unternehmen. Es ist aber nur ein Puzzlestück im gesamten Bild. Die Definition eines passenden Sicherheitskonzepts stellt eine grosse Herausforderung dar, die Unternehmen in der Regel ohne Unterstützung von externen Cyber-Experten nicht bewältigen können. Hier bietet sich die Chance für Partner, eine Vertrauensbasis zu schaffen, um Unternehmen mit einem gesamtheitlichen Ansatz beraten zu können.

Cornelia Lehle
Head of Sales DACH, G Data

Weshalb sind Security-Awareness-Trainings wichtig? Dass man nicht auf irgendwelche komischen Links klicken sollte, weiss man doch unterdessen.
Cornelia Lehle: Nichts ändert sich schneller als Angriffsszenarien auf Unternehmensnetzwerke. Daher reichen weder einmalige Schulungen zu aktuellen Bedrohungen noch kurze Trainingsvideos zu den Merkmalen von Phishing-Mails aus. Kontinuierliche Schulungen schärfen das Sicherheitsbewusstsein der Mitarbeitenden und sorgen für ein langfristig höheres Know-how hinsichtlich der IT-Security.

Was ist der Schlüssel zum Erfolg bei Awareness-Trainings?
Awareness-Trainings sind kein Sprint, sondern ein Langstreckenlauf. Wer den Themenkomplex vollständig abdecken will, benötigt einen umfassenden und langfristig ausgelegten Lehrplan sowie zeitgemässe Lernmethoden. Nur so lässt sich Wissen bedarfsgerecht vermitteln. Um den Lernerfolg zu maximieren und die Inhalte nachhaltig bei den Mitarbeitenden zu verankern, braucht es ausserdem Kontinuität und Aktualität.

Was müssen Reseller selbst können/wissen, um derartige Trainings erfolgreich anzubieten?
Idealerweise kennen Reseller die Themen und Inhalte im Detail und haben selbst das Training absolviert. Für die Integration der Awareness-Trainings braucht es kein zusätzliches Wissen. Die Unternehmen haben die Möglichkeit, unsere Trainings als Full-Service mit einem Learning Management System in ihr System zu integrieren. Unternehmen, die bereits eine eigene Lernplattform nutzen, können unsere Schulungen über eine Schnittstelle in ihr eigenes System einbetten. Wir sind also sehr flexibel mit unseren Lösungen und unterstützen damit unsere bestehenden Reseller und alle, die es noch werden wollen, ideal.

Inwiefern führt das Angebot von Awareness-Trainings zu weiterem Business für Reseller?
Fachhändler stärken mit diesem noch sehr jungen Angebot ihre Rolle als vertrauenswürdiger Dienstleister und können als strategischer Partner mit ihren Kunden eine langfristige Geschäftsbeziehung aufbauen, beziehungsweise diese fortsetzen. Denn der Bedarf nach umfassenden IT-Sicherheitskonzepten inklusive Dienstleistungen aus einer Hand wird eher zu- als abnehmen.

Franco Cerminara
Chief Consulting Officer, Infoguard

Weshalb sind Security-Awareness-Trainings wichtig? Dass man nicht auf irgendwelche komischen Links klicken sollte, weiss man doch unterdessen.
Franco Cerminara: Das initiale Ziel von Cyberattacken ist immer häufiger der «Mensch». Wieso mühsam Sicherheitssysteme knacken, wenn ein gezieltes Phishing-E-Mail ausreicht? Viele Mitarbeitende erkennen solche E-Mails jedoch nicht. Genau hier setzt Security Awareness an, um die Mitarbeitenden zu schulen und zu sensibilisieren. Ziel ist es, Risiken zu identifizieren, Angriffe zu erkennen und richtig zu reagieren.

Was ist der Schlüssel zum Erfolg bei Awareness-Trainings?
Für einen maximalen Lernerfolg sollten Beispiele verwendet werden, mit denen Mitarbeitende im Alltag konfrontiert sind. Die Risiken können je nach Tätigkeit sehr verschieden sein. Darauf gilt es einzugehen. Zudem muss den Mitarbeitenden klar werden, dass sie einen bedeutenden Beitrag zur Sicherheit leisten.

Was müssen Reseller selbst können/wissen, um derartige Trainings erfolgreich anzubieten?
Security-Awareness-Trainings bestehen nicht nur aus einem einmaligen Workshop. Zentral ist ein mehrstufiges Konzept, das technisch sowie kommunikativ auf die Mitarbeitenden zugeschnitten ist.

Inwiefern führt das Angebot von Awareness-Trainings zu weiterem Business für Reseller?
Ausser dem Faktor Mensch gehören zu einem effektiven Sicherheitsdispositiv Prozesse und Technologien, die bei uns ebenso zum Business gehören. Dazu setzen wir auf einen 360-Grad-Ansatz – sprich, Consulting inklusive Penetration Testing, Security-Lösungen sowie Cyber-Defence-Services, um unsere Kunden 24x7 zu überwachen, Angriffe abzuwehren und im Notfall unterstützen zu können.

Christian Meier
Head of Business Security Consulting, Ispin

Weshalb sind Security-Awareness-Trainings wichtig? Dass man nicht auf irgendwelche komischen Links klicken sollte, weiss man doch unterdessen.
Christian Meier: Security Awareness ermöglicht den Unternehmen, aktiv statt reaktiv zu agieren. Es wird immer Schwachstellen geben, die nicht zeitnah geschlossen werden können oder unbekannt sind. Hier kommt der Faktor Mensch als wichtigste beziehungsweise letzte Abwehrlinie ins Spiel. Schulungen zur Erhöhung des Sicherheitsbewusstseins helfen dabei, Sicherheitsverletzungen zu verhindern.

Was ist der Schlüssel zum Erfolg bei Awareness-Trainings?
Eine erfolgreiche Sensibilisierung sollte sowohl die eigenen Schwächen und den Wissensstand der Mitarbeitenden berücksichtigen als auch die spezifischen Gefahren und Risiken für das Unternehmen. Die Schulungen sollten konkrete Schlüsselpersonen (HR, Finance, IT-Admins) berücksichtigen und individuell gestaltet sein. Zudem ist es wichtig, die Auswirkungen und die Wirksamkeit eines Sicherheitsprogramms zu verstehen.

Was müssen Reseller selbst können/wissen, um derartige Trainings erfolgreich anzubieten?
Zunächst muss man die Realität kennen, die unsere Berater tagtäglich bei Kunden erleben. Wenn die Sicherheitsschulungen nicht aktuell sind und sich nicht auf «echte» Fälle beziehen, ist eine erfolgreiche Sensibilisierung höchst unwahrscheinlich. Andererseits müssen die Trainings auch Spass machen. Dies erfordert eine gute Portion Kreativität und ein Gespür für Trends, wie zum Beispiel «Gamification».

Inwiefern führt das Angebot von Awareness-Trainings zu weiterem Business für Reseller?
Awareness-Schulungen müssen individuell gestaltet sein und setzen Kenntnisse über die Unternehmenskultur, den Reifegrad der Informationssicherheit und deren Organisation voraus. Dieses bessere Kundenverständnis ermöglicht es, Schwachpunkte (organisatorisch, prozessual oder technologisch) besser zu erkennen und entsprechende Unterstützungen oder Beratungen anbieten zu können. Beispiel: fehlende Prozesse beim Incident Response im Fall, dass Mitarbeitende auf bösartige Betrugsversuche reinfallen.

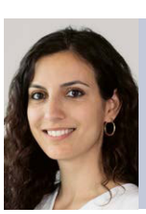
Palo Stacho
Head of Operations, Lucy Security

Weshalb sind Security-Awareness-Trainings wichtig? Dass man nicht auf irgendwelche komischen Links klicken sollte, weiss man doch unterdessen.
Palo Stacho: Der überwältigende Anteil der erfolgreichen Hacks nimmt immer noch seinen Anfang bei unachtsamen Mitarbeitenden. Es ist möglich, dass inzwischen viele Leute bei «komischen Links» argwöhnisch werden. Doch es gibt gefährliche Links, die auf den ersten Blick ausgesprochen legitim aussehen (URL-Spoofing) und wir sollten nicht vergessen, dass es immer noch Browser gibt, welche die Webadresse gar nicht anzeigen. Obendrein ist es sehr einseitig, die Schulungsbemühungen lediglich auf dubiose Links auszurichten. Gefahren können auch von Dateianhängen in E-Mails, von SMS, USB-Sticks und anderen Social-Engineering-Techniken ausgehen.

Was ist der Schlüssel zum Erfolg bei Awareness-Trainings?
Zunächst sollte man sich überlegen, was in diesem Kontext «Lernerfolg» heisst: Maximaler Lernerfolg bedeutet nämlich, dass das Personal im Internet ein sicheres Verhalten an den Tag legt! So etwas geht weit über eine Schulungsmassnahme hinaus, das ist ein Innovationsvorhaben. Für uns ist es erwiesen, dass der Erfolg nur dann erreicht werden kann, wenn ein ständiges Awareness-Programm betrieben wird, das einen positiven Charakter aufweist, das Engagement des Einzelnen fördert und messbare Ziele beinhaltet. Die im Rahmen des Programms durchgeführten Phishing-Tests haben realitätsnah zu sein. Die Lernmodule sind abwechslungsreich und unterhaltsam zu gestalten und zwingend personalisiert, sprich die Schulung ist in den Kontext des Mitarbeiters und der Firma eingebettet.

Was müssen Reseller selbst können/wissen, um derartige Trainings erfolgreich anzubieten?
Standardisierte Nullachtfünfzehn-Phishingtests oder Awareness-Trainings erzielen wenig Nachhaltigkeit. Natürlich sollte das zum Grundangebot gehören. Die Reseller sollten aber Lösungen einsetzen, die eine Individualisierung und Anpassbarkeit der Trainings ermöglichen.

Inwiefern führt das Angebot von Awareness-Trainings zu weiterem Business für Reseller?
Das Schulungsbedürfnis in Wirtschaft und Bevölkerung ist enorm! Cybersecurity Awareness geht jeden etwas an, mehr muss man dazu nicht sagen.



Isil Günalp
Product Manager IT Security, Digicomp Academy

Weshalb sind Security-Awareness-Trainings wichtig? Dass man nicht auf irgendwelche komischen Links klicken sollte, weiss man doch unterdessen.
Isil Günalp: Die Statistik zeigt ein klares Gegenbild: Cyberkriminalität ist im Aufwind. Warum? Weil Wissen nicht mehr ausreicht. Wir brauchen ein erhöhtes Sicherheitsbewusstsein, das sich in das Arbeitsgedächtnis einprägt. Ein wirksames, auf die Bedürfnisse des Unternehmens zugeschnittenes Awareness-Programm ist deshalb unverzichtbar. Gut geschulte Mitarbeitende kennen die besten Taktiken, um eine Cyberattacke zu verhindern, darauf zu reagieren und sich davon zu erholen. Eine Sensibilisierung der Belegschaft verringert das Gesamtrisiko des Unternehmens und ebnet auch den Weg in eine GDPR-konforme Zukunft. Das führt zudem zu einem besseren Ruf des Unternehmens, verlässlichen Beziehungen mit Lieferanten und Kunden und letztlich zu mehr Business.

Was ist der Schlüssel zum Erfolg bei Awareness-Trainings?
Security muss Spass machen! Die Mitarbeitenden sollten ihr Wissen mit Simulationen und spielerischen Angriffsszenarien testen. Hilfreich ist auch, das vermittelte Wissen privat nutzbar zu machen, denn die Mitarbeitenden begegnen zuhause denselben Problemen wie im Geschäft. Dabei ist zu beachten, dass das Wissen und der Umgang der Mitarbeitenden sehr unterschiedlich sind. Eine einfache, klare und verständliche Botschaft in einem Format zu vermitteln, das von der Zielgruppe leicht verstanden wird, sollte die Voraussetzung für jedes Training sein. Das «Know» in ein «How» zu verwandeln ist dann der Schlüssel zum Erfolg. Sie sollten wissen, dass sie die Macht haben, Cyberangriffe zu stoppen.

Was müssen Reseller selbst können/wissen, um derartige Trainings erfolgreich anzubieten?
Awareness-Schulungen liegen im Trend. Gute und vertrauenswürdige Reseller dafür zu finden, ist deshalb schwierig geworden. Ein guter Partner sollte auf jeden Fall in der Weiterbildungsbranche etabliert sein, sich auf IT-bezogene Themen spezialisiert haben und einen gewissen Marktanteil in diesen Themen besitzen. Wenn darüber hinaus ein steigendes Marktwachstum zugesichert werden kann, dann sollte einer langfristigen Zusammenarbeit nichts im Wege stehen.

Inwiefern führt das Angebot von Awareness-Trainings zu weiterem Business für Reseller?
In der ersten Trainingseinheit werden oft zusätzliche Schwachstellen und Bedrohungen im Unternehmen aufgedeckt, die nicht in einer einzigen Schulung vermittelt werden können. Fortlaufende Schulungen können dabei helfen, die Herausforderungen in verschiedenen Abteilungen gezielt anzugehen. Wenn zum Beispiel im Buchungsprozess eine Schwachstelle auf der Website festgestellt wird, ist es sicherlich sinnvoll, die Website auf die Attraktivität für Cyberkriminelle zu prüfen und die Webentwickler entsprechend zu schulen. Und wenn die Teilnehmenden zufrieden sind, betreiben sie automatisch positives Mundpropaganda-Marketing, was auch zu mehr Business führt.

Alex Faes
Network & Security Consultant, RedIT Services

Weshalb sind Security-Awareness-Trainings wichtig? Dass man nicht auf irgendwelche komischen Links klicken sollte, weiss man doch unterdessen.
Alex Faes: Ein IT-Sicherheitssystem ist nur so stark wie ihr schwächstes Glied – und dabei geht es nicht nur um Technologien und Prozesse, sondern insbesondere um den Risikofaktor Mensch. Die Minimierung dieser potenziellen Schwachstelle ist ein essenzieller Baustein jeder IT-Sicherheitsstrategie. Durch Social Engineering wird aus einem komischen Link rasch ein unverdächtiger Link. Phishing-Mails sind längst nicht der einzige Angriffsvektor, der in einem Security-Awareness-Training behandelt wird.

Was ist der Schlüssel zum Erfolg bei Awareness-Trainings?
Awareness-Trainings benötigen die volle Aufmerksamkeit der Teilnehmenden. Viele Angriffe zielen nämlich auf die Unachtsamkeit der IT-Anwender ab. Deshalb sind Präsenzschulungen oft nachhaltiger als Onlineschulungen, wo häufig nebenbei noch andere Tätigkeiten ausgeübt werden beziehungsweise die Teilnehmenden schneller abgelenkt sind. Beim Training sollte eine Atmosphäre herrschen, in der sich die Teilnehmenden nicht genieren müssen, Fragen zu stellen.

Was müssen Reseller selbst können/wissen, um derartige Trainings erfolgreich anzubieten?
Ausser didaktischen Fähigkeiten ist die Kundennähe wichtig, um die Trainings individuell nach Branche, Kultur und Sprache des Kunden durchzuführen. Die Unterlagen und Praxisbeispiele müssen permanent den aktuellen Cyberrisiken angepasst werden.

Inwiefern führt das Angebot von Awareness-Trainings zu weiterem Business für Reseller?
Der Referent kann seine Kompetenz persönlich der ganzen Belegschaft aufzeigen. Wo erhält man sonst diese Einstiegschance. Ein IT-Sicherheitssystem ist nur so stark wie ihr schwächstes Glied – welches ist nach der Schulung jetzt das schwächste Glied?