G DATA academy

SECURITY AWARENESS TRAININGS

WIE ONLINE-KURSE UND SPIELERISCHE ANSÄTZE DEN LERNERFOLG STEIGERN

G DATA academy

INHALT

UNWISSENHEIT SCHÜTZT NICHT VOR CYBERATTACKEN

Mit Security Awareness Trainings das Bewusstsein für Cyberrisiken verbessern und Unternehmen vor Angriffen schützen

Autofahren und IT-Sicherheit haben mehr gemeinsam, als es auf den ersten Blick scheint. In beiden Fällen schützen technologische Maßnahmen vor schweren Unfällen oder deren Folgen. Beim Auto sind es Airbags, Gurte oder Bremsassistenten, bei Computern und Netzwerken Endpoint Protection, Firewall und Back-ups. Aber die Realität führt uns tagtäglich vor Augen, dass wir Menschen ebenfalls eine zentrale Rolle spielen, wenn es darum geht, Unfälle zu vermeiden. Ein vergessener Schulterblick, ein falsch eingeschätzter Abstand und schon kracht es. Richtiges Verhalten im Straßenverkehr lernen wir in der Regel in der Fahrschule, aber richtiges Verhalten im digitalen Raum?

Das vorliegende White Paper beschäftigt sich mit der Frage, welche Rolle Mitarbeitende beim Thema IT-Sicherheit spielen (Spoiler: eine sehr wichtige) und wie E-Learnings helfen, das Bewusstsein der Menschen für einen sicheren Umgang mit der IT zu verbessern.

AKTUELLE BEDROHUNGSLAGE: ATTACKEN IM SEKUNDENTAKT

Die vergangenen Jahre haben uns eindrücklich vor Augen geführt, wie fragil die IT-Sicherheitslage ist – nicht nur in Deutschland, sondern weltweit nutzten Cyberkriminelle die Verunsicherung der Menschen infolge der Corona-Pandemie aus. Laut einer Bedrohungsanalyse von G DATA CyberDefense stieg die Zahl der abgewehrten Angriffsversuche im vierten Quartal 2021 um 25 Prozent – im Vergleich zum dritten Quartal. Das zeigt: Cyberkriminelle haben schnell erkannt, dass die Homeoffice-Situation neue Schwachstellen mit sich bringt. Und diese nutzen sie aus. Ebenso wie andere Schwachstellen: Kritische Sicherheitslücken, fehlende Updates oder unvorsichtige Angestellte stehen meist am Anfang einer erfolgreichen Attacke.

Auffällig ist, dass Cyberkriminelle auf bewährte Schadsoftware setzen, die zum Teil schon seit mehreren Jahren im Einsatz ist, aber ständig weiterentwickelt wird. Wie groß die Gefahr ist, belegen folgende Zahlen:

- Mehr als 23,7 Mio. verschiedene Malware-Samples entdeckten die Cyber-Defense-Experten von G DATA.
- Gegenüber dem Vorjahr ist dies ein Anstieg von 47 Prozent.
- Pro Minute veröffentlichten Cyberkriminelle 45 neue Versionen einer Schadsoftware.

Eine aktuelle Umfrage bei mittelständischen Unternehmen von G DATA belegt: Kleinen und mittleren Unternehmen – beziehungsweise deren Mitarbeitenden – fehlt ein ausreichendes Bewusstsein für Cybergefahren. Sie sehen sich trotz der immens gestiegenen Bedrohungslage selbst nicht als interessante Ziele für Cyberkriminelle. Die Folgen dieser Fehleinschätzungen sind fatal und führen dazu, dass sich die Unternehmen unzureichend gegen Angriffe schützen und IT-Sicherheitsvorfälle sie umso härter treffen.

Fehlendes Bewusstsein und der Mangel an nötigen Ressourcen stehen den befragten Unternehmen massiv im Weg. Rund ein Viertel der befragten KMU geben als Grund an, dass ihr Unternehmen kein interessantes Angriffsziel für Cyberkriminelle sei.

SCHWACHSTELLE MENSCH

Eine Umfrage des Kriminologischen Forschungsinstitutes Niedersachsen kommt zu dem Ergebnis, dass 74 Prozent der Malware-Attacken mit einer Phishing-Mail starten. Ein falscher Klick eines Mitarbeitenden reicht aus und das Unheil nimmt seinen Lauf. Diese Nachrichten enthalten oft einen schädlichen Dateianhang oder einen Link zu einer Webseite, über die Schadcode ausgeliefert oder vertrauliche Daten „abgefischt“ werden. Die Folgen können die Existenz jedes Betriebes bedrohen. Zum finanziellen Schaden durch den tage- oder wochenlangen Produktionsausfall gesellt sich auch der Imageschaden, wenn vertrauliche Kundendaten wie Login-Information oder Zahlungsdaten in die Hände Dritter geraten.

Welche Folgen das Fehlverhalten eines einzelnen Mitarbeitenden haben kann, zeigt folgendes Beispiel: Im Februar 2020 legte eine Cyberattacke den Betrieb des Elektrogroßhändlers Möhle in Münster drei Wochen lang lahm. Ein Mitarbeiter hatte einen mit Schadsoftware infizierten E-Mail-Anhang geöffnet, sodass die Angreifer auf das Netzwerk zugreifen und es verschlüsseln konnten. Sämtliche Bildschirme im Unternehmen wurden weiß und zeigten nur noch einen Warnhinweis. Erschwerend kam hinzu, dass das Unternehmen aufgrund eines Fehlers im Backup-System seine Daten nicht einfach wiederherstellen konnte. Die Firma sah sich gezwungen – entgegen dem Ratschlag der Kriminalpolizei – mit den Tätern zu verhandeln. Am Ende musste Möhle 120.000 Euro Lösegeld zahlen. Ohne diese Zahlung hätten sie keinen Zugriff auf die Daten erhalten, was die Existenz des Unternehmens gefährdet hätte.

Dass Phishing ein einfacher und beliebter Angriffsvektor für Cyberkriminelle ist, führt auch bei vielen Angestellten zu Verunsicherung. Das belegt eine Untersuchung der Initiative Deutschland sicher im Netz e.V.. Mehr als 56 Prozent der Befragten gaben an, dass sie beim Öffnen einer E-Mail verunsichert sind.

CEO-Fraud: Überfall per Mail

PB

peter.b.kohlemacher@kohlemacher.ru
An: brigitte@kohlemacher.de

Hallo Brigitte,
kannst du bitte folgende Überweisung für unseren Kunden Hilf & Reich tätigen:
Summe: 17.500 Euro
IBAN: DE12 3456 6543 0000 1234 56
Verwendungszweck: Rückzahlung für Fehlbuchung
Bei Hilf & Reich hat vor sechs Wochen eine neue Buchhalterin angefangen und die hat bei der Buchung einen Fehler gemacht. Aber das können wir ja schnell zurückbuchen.

Herzlichen Dank für deine Hilfe
Peter

Geschäftsführer

Brigitte Ziffrich, seit vielen Jahren Chef-Buchhalterin bei der Steuerberatung „Kohlemacher & CO.“, ist schon beim ersten Lesen misstrauisch. Seit wann duzt ihr Chef sie? Obwohl beide seit vielen Jahren vertrauensvoll miteinander arbeiten, siezen sie sich – wie alle 17 Mitarbeitenden auch. Beim zweiten Blick fällt ihr auf, dass die Signatur ihres Chefs anders aussieht als sonst: Die Schrift ist anders und auch das Firmenlogo ist verzerrt. Sie druckt die Mail aus und spricht Peter Kohlemacher direkt an. Seine Antwort: „Nein, diese Mail stammt nicht von mir!“

Gemeinsam prüfen die beiden weitere Details der Meldung. Ein Vergleich der IBANs zeigt, dass es sich nicht um das reguläre Firmenkonto von Hilf & Reich handelt. Und auch die Mail-Adresse des Absenders ist falsch, sie lautet: peter.b.kohlemacher@kohlemacher.ru.

Das Unternehmen in diesem Beispiel hat Glück im Unglück und ist nicht einem sogenannten CEO-Fraud zum Opfer gefallen. Bei dieser Betrugsmasche geben sich Kriminelle als Geschäftsführung oder Führungskraft eines Unternehmens aus. Sie fordern in gefälschten E-Mails entsprechend berechtigte Mitarbeitende aus der Buchhaltung oder dem Rechnungswesen dazu auf, größere Summen von Unternehmenskonten zu überweisen. Im Vorfeld sammeln die Täter viele Informationen über das anzugreifende Unternehmen und gelangen so an das notwendige Insiderwissen für ihre Betrugsmasche. Dieses Wissen setzen sie beim Angriff ein und verursachen dabei großen finanziellen Schaden.

DIE ROLLE DES MENSCHEN BEI DER IT-SICHERHEIT

Corona hat uns als Gesellschaft dazu gezwungen, uns mit neuen Begebenheiten auseinanderzusetzen: Wie funktioniert Arbeit außerhalb meines Büros? Wie gehe ich mit Kollegen um, wenn ich diesen ausschließlich virtuell begegne? Wie strukturiere ich meinen Arbeitstag, den ich in meinen eigenen vier Wände verbringe? An einem Ort, der eigentlich mit Wörtern wie Feierabend oder Entspannung, aber nicht zwingend mit Arbeit verknüpft ist? Vor allem die aktuellen Begebenheiten zwingen uns dazu, sich mit diesen Fragen auseinanderzusetzen. Wir sind quasi direkt von den Auswirkungen der Pandemie betroffen.

Wo es direkte Betroffenheit gibt, ist ein Äquivalent nicht fern – nennen wir es „indirekte“ Betroffenheit. Zu dieser Kategorie gehören etwa Fragen rund um unsere digitale Sicherheit. Warum? Die Antwort darauf ist einfach: In Zeiten eines normalen Büroalltags hat unser Arbeitgeber beziehungsweise dessen IT-Abteilung Sorge dafür getragen, dass wir und unser Arbeitsplatz digital geschützt sind. Die Arbeitnehmenden haben sich also aus einem Gefühl heraus, darauf verlassen, dass sobald sie das Büro betreten, die (digitale) Sicherheit durch die Sorgfaltspflicht des Arbeitgebers gewährleistet wird. Dabei gibt es neben den offensichtlichen Endpoint-Protection-Lösungen, Firewalls und Zwei-Faktor-Authentifizierungen auch weitere Sicherheitsvorkehrungen wie etwa Zugangsbeschränkungen und Identifikationsmechanismen. Diese sollen klar regeln, wer was darf oder eben nicht darf. Die Maßnahmen zielen darauf ab, dass etwa unternehmenskritische Informationen nicht in unberechtigte Hände fallen. Diese Liste ist natürlich nicht vollständig.

Grundsätzlich lässt sich festhalten: Mit Fragen rund um die digitale Sicherheit und um die Sicherheit unserer Informationen mussten wir uns im normalen beruflichen Kontext nur bedingt auseinandersetzen. Ein Großteil der Angestellten arbeitet in der Überzeugung, dass der jeweilige Arbeitgeber das vor Ort schon ganz gut im Griff hat.

Aber: Wie steht es um die IT-Sicherheit im Homeoffice? Wie verhalten sich Mitarbeitende in einer Situation, in der sich unsere Work-Life-Balance stark verändert hat, weil wir Arbeit und Privatleben weniger strikt trennen. In der sich einzelne Personen mit Fragen auseinandersetzen mussten, die sonst andere Fachleute für sie kompetent festlegen: Wie schütze ich unternehmenskritische Daten, wenn ich mich eben nicht in meiner altbekannten, kontrollierten Firmen-Bubble, also in meinem Büro, befinde?

Zyniker sprechen schon länger davon, dass das größte Risiko unmittelbar vor dem Bildschirm sitzt. Dieser, zugegeben, etwas in die Jahre gekommene Satz, hat in Zeiten von Corona nochmals stark an Gewichtung (zurück-)erhalten. Ebenfalls verdeutlicht er einen Umstand fast schon in Reinkultur: Die Rolle des Menschen bei der IT-Sicherheit war noch nie wichtiger!

Aber warum ist das so?

Ein Grund: Wir müssen uns mit einer unbekannten Situation auseinandersetzen. Wir arbeiten in der eigenen Wohnung, umgeben von unserer Familie und oder Mitbewohner*innen, die aber nicht zum Kollegenkreis gehören. Ein eigenes Arbeitszimmer steht nicht immer zur Verfügung, sondern wir arbeiten am Küchentisch oder im Wohnzimmer. Die Informationen auf dem Bildschirm sind nicht für die Augen der Familie/Mitbewohner*innen und die Telefonate nicht für ihre Ohren bestimmt. Die Unterlagen aus dem Büro können wir auch nicht einfach über den Papierkorb entsorgen. Im Büro stehen dafür in der Regel gesonderte, abgeschlossene Boxen oder Schredder bereit. Diese drei Beispiele sollen eines verdeutlichen: Damit wir auch in Zukunft sicher mit unternehmenskritischen Daten arbeiten, braucht es ein großes Umdenken. Ein Umdenken, welches keine Endpoint-Protection-Lösung für uns übernehmen kann. Die Arbeitswelt ist seit Beginn der Pandemie eine andere geworden und Arbeiten im Homeoffice gehört in vielen Unternehmen zum neuen Alltag.

Damit auch in dieser neuen Arbeitssituation die digitale Präsenz und alle Daten sicher bleiben, braucht es nicht nur eine aktuelle Sicherheitslösung. Es braucht ein neues Bewusstsein darüber, dass der Mensch die zentrale Rolle einnimmt, um die eigenen, aber auch unternehmenskritische Daten zu schützen.

Mit dieser Erkenntnis stellt sich eine weitere zentrale Frage: Wie gelingt dieses Umdenken? Anders gefragt: Was müssen Unternehmen tun, damit ihre Mitarbeitenden, aber auch Angestellte von Dienstleistern, sich neue Verhaltensweisen angewöhnen? Damit sie auch außerhalb des Büros wichtige Daten und Informationen schützen?

Dies kann gelingen, indem wir das menschliche Verhalten updaten – mit sogenannten Security Awareness Trainings. Diese Schulungen stellen den Menschen in den Mittelpunkt, nicht die Technik. Sie veranschaulichen, wie wir nicht nur unsere Arbeitgeber und seine Dateien, sondern auch unsere eigene private digitale Präsenz vor Gefahren und Angriffen schützen. Mit diesen Trainings lässt sich gezielt nicht nur Aufmerksamkeit im wörtlichen Sinne, sondern ein generelles Umdenken erreichen und Mitarbeitende verstehen, welchen Beitrag sie für die IT-Sicherheit leisten können und müssen.

SECURITY AWARENESS TRAININGS

Um es klar zu sagen: Awareness Trainings sind kein Sprint, sondern ein Langstreckenlauf, denn das Sicherheitsbewusstsein der Mitarbeitenden muss sich langfristig ändern. Hinzu kommt, dass das Themenspektrum umfangreich ist, sodass es eines umfassenden und langfristig ausgelegten Lehrplans bedarf. So gehört der sichere Einsatz mobiler Arbeitsgeräte im Arbeitsalltag ebenso dazu wie das Erstellen von sicheren Passwörtern oder der Umgang mit verdächtigen E-Mails. Ein weiteres Thema: Die bloße Existenz eines IT-Notfallplans verhindert keinen Cyberangriff. Mitarbeitende müssen diesen kennen und reagieren.

Folgende Themengebiete sollten durch Security Awareness Trainings abgedeckt sein:

- Die neue Art zu arbeiten – Arbeiten außerhalb des Büros und an öffentlichen Orten
- Risikomanagement und Passwörter – Sichere Passwörter erstellen und richtig einsetzen
- Phishing und Malware – Wie Mitarbeitende Malware und Phishing-Versuche erkennen
- Klassifizierung der zu bearbeitenden und zu speichernden Informationen – Um welche Daten handelt es sich? Wie werden Informationen klassifiziert und warum?
- Arbeiten in der Cloud – Social Media und sicheres Arbeiten in der Cloud
- Sicherheitsvorfälle und Reports – Cyber-Security-Vorfälle und Zugangskontrollen
- Social Engineering – Wie Hacker Mitarbeitende für ihre Angriffe manipulieren
- Mobile Geräte – Smartphones, Tablets und Co. in der Arbeitswelt sicher einsetzen
- Rechtliche Rahmenbedingungen - DSGVO, AGG, Compliance, Kartellrecht und Arbeitsschutz
- Ransomware, Remote Access Trojaner, Keylogger und Rootkits – Welche Schadsoftware bedroht Unternehmen?

MEHR AUFMERKSAMKEIT DANK E-LEARNING

Cyberkriminelle gehen bei ihren Attacken immer gezielter vor und sprechen ihre Opfer direkt an. Die Erfolgschancen stark individualisierter Angriffe sind hier deutlich höher als bei einem Massenangriff.

Der Grund dafür? Menschliches Verhalten lässt sich auf verschiedene externe Trigger zurückführen. Das sind externe Einflüsse, die bei Menschen ein konkretes Verhalten auslösen. Zu diesen Auslösern gehört etwa Neugier, wie das folgende Beispiel zeigt:

Kurz vor den Weihnachtsferien landet eine Mail im Postfach von Tina, Sachbearbeiterin in einem Versicherungskonzern. Der Inhalt ist brisant: Der Absender teilt mit, dass er auf der letzten Firmenfeier kompromittierende Fotos von Tina gemacht hat. Er bittet sie, sich diese anzusehen und sich zu melden, damit diese nicht weiterverbreitet werden. Tina überlegt fieberhaft, was auf der Weihnachtsfeier vor zwei Wochen passiert ist und ist geneigt, den Link in der Mail anzuklicken. Hier handelt es sich um eine Phishing-Mail. Die Fotos existieren nicht und doch ist der Wunsch nachvollziehbar, die Situation mit einem Klick auf den Link zu klären. Warum das so ist? Warum klicken viele Menschen auf diese oder vergleichbare Nachrichten?

In dem beschriebenen Fall ist Druck der treibende Trigger. Grundsätzlich werden zumeist mehrere Trigger miteinander verknüpft. Auch der bereits angesprochene Trigger Neugier kommt immer wieder zum Einsatz. So gering die Wahrscheinlichkeit auch ist, es könnte unter Umständen doch wahr sein. Weitere Auslöser sind Hilfsbereitschaft oder Gier. Wer hatte nicht schon eine E-Mail in seinem Postfach, die ihm oder ihr einen Millionengewinn oder eine Erbschaft in Aussicht stellte?

Das ist es also nicht verwunderlich, wenn Menschen den falschen Link anklicken, weil er oder sie erfahren will, ob der Milionengewinn echt ist oder nicht.

Übrigens: Tina hat den Link in der Mail nicht angeklickt, sondern die Mail an einen Kollegen in der IT-Abteilung weitergeleitet. Nach einer kurzen Prüfung konnte er Tinas Verdacht bestätigen: Die Mail war ein Phishing-Versuch.

Das Beispiel belegt, welche psychologischen Tricks Cyberkrimielle nutzen, um Menschen zu ungewollten Handlungen zu verleiten. Wichtig in diesem Zusammenhang: Das Opfer ist nicht der Schuldige!! Es wird zu diesen Taten durch verschiedenen psychologische Tricks zum Handeln verleitet.

Die gute Nachricht: Unternehmen können sich und ihre MItarbeiter*innen gegen diese hinterhältigen Angriffe schützen: MIt Security Awareness Trainings.

Keine technischen Schutzmaßnahmen, wie etwa eine Sicherheitslösung, kann Nutzer*innen vollumfänglich vor zum Beispiel Phishing-Angriffen schützen. Es liegt an den Menschen und vor allem an ihrem Sicherheitsbewusstsein, solche Angriffsformen frühzeitig zu erkennen und abzuwehren.

Moderne E-Learnings vermitteln den Lernenden ein umfangreiches Wissen rund um die verschiedenen Angriffe und Angriffsformen. Die Lerneinheiten erklären praxisnah, wie Angriffe im Arbeitsalltag ablaufen, worin deren Gefahr besteht und wie sich Angestellte davor schützen können. Moderne E-Learnings im Bereich Security Awareness sind dynamisch und vor allem kurzweilig in Lernreihen aufgebaut. Damit können Lernende jederzeit auf das Training zugreifen und sich schnell und unkompliziert weiterbilden.

Fazit: Es gibt keinen ausreichenden technischen Schutz, der Anwender*innen vor allen Cybergefahren schützen kann. Vor allem Phishing-Attacken umgehen die technischen Schutzmechanismen, indem sie den Menschen direkt ins Visier nehmen.

Aber: Mit einem umfangreichen Wissen durch Security Awareness Trainings über die Methoden und Ziele von Angreifern, sind Mitarbeitende gewappnet, um nicht auf die Betrugsversuche reinzufallen.

E-Learnings, beziehungsweise Security Awareness Trainings machen aus Anwender*innen nicht nur die letzte, sondern auch die effektivste Verteidigungslinie gegen Cyberangriffe.

GLEICHES WISSEN FÜR ALLE

Security Awareness Trainings zielen darauf ab, Lerner*innen in die Lage zu versetzen, Gefahren und Angriffe zu erkennen, die sie oder ihn direkt im Visier haben und gegen die es nur einen unzureichenden technischen Schutz gibt. Digitale Fortbildungen sind im Wandel und entwickeln sich stetig weiter. Mit wachsendem technologischen Fortschritt und der immer weiter voranschreitenden Digitalisierung haben sich nicht zuletzt auch E-Learnings in ihrem Wesen weiterentwickelt. Die Zeiten, in denen Mitarbeitende teilweise 60 Minuten lange, spärlich animierte, unvertonte, staubtrockene E-Learnings absolvieren sollten, sind vorbei. Der Lerntransfer ging bei diesem Ansatz gegen Null.

Der Grund dafür: Immer wieder lenken uns E-Mails, Telefonate, Kollegen, Nebenaufgaben oder andere Geräusche ab. Es fällt also zunehmend schwerer, sich für eine längere Zeitspanne zu konzentrieren und ungestört zu arbeiten. Aufmerksamkeit wird immer mehr zu einer knappen und wertvollen Ressource. Denn für viele Unternehmen ist Lernzeit gleich Arbeitszeit. Für Security Awareness Trainings heißt das: Sie müssen ab Sekunde eins den Lerntransfer maximieren. „Micro-Learnings“ tragen diesem Umstand Rechnung und sorgen dafür, kleine Lerneinheiten leichter in den modernen Arbeitsalltag zu integrieren. Hinzu kommt: Bereits nach dem erstmaligen Abschluss lassen sich Micro-Learnings dazu nutzen, Fragen, die im Arbeitsalltag spontan auftauchen, zu beantworten. Indem Lernende diese wieder aufrufen, sobald es erforderlich ist. Dagegen verlieren E-Learning-Formate, die 45 Minuten und länger dauern, zunehmend an Akzeptanz. Unternehmen und Privatpersonen greifen immer mehr auf kleine und smarte Mobile-Learning-Angebote zurück.

Moderne E-Learnings richten sich nach den Bedürfnissen und den individuellen Voraussetzungen der Lernenden. Zentrale Aspekte eines zeitgemäßen E-Learnings sind:

- kurze Einheiten
- funktionierendes (charakterbasiertes) Storytelling
- Lernstandspeicherung
- direkte Ansprache des Lernenden
- viel Interaktion zwischen Training und Anwender*innen
- eine direkte Wissensvertiefung im Training selbst

Gepaart mit der Tatsache, dass moderne E-Learnings auf mobilen Endgeräten nutzbar sind, versetzen sie die Lernenden in die Lage, immer und überall lernen zu können. Hier gilt das Motto „Lebenslanges Lernen hört nie auf.“ Heißt: Anstelle auf einer Dienstreise in der Bahn seine Zeit damit zu verbringen, gedankenverloren aus dem Fenster zu schauen, können Menschen die Zeit auch produktiv nutzen und an ihrem Sicherheitsbewusstsein arbeiten. Dank einer einfachen Benutzeroberfläche können Lernende direkt an der Stelle fortfahren, an der sie aufgehört haben. Für jede abgeschlossene Lerneinheit erhalten Lernende zudem ein Zertifikat. Durch die Nutzung von Gamification-Elementen und einer spannenden Erzählweise in den Trainings, kommt auch der Spaß dabei nicht zu kurz.

Für ein zentrales Thema wie IT-Sicherheit bedeutet dies: Der Mensch ist nur dann effektiv gegen Cyberangriffe gewappnet, wenn das notwenige Wissen um den Schutz auch ständig vorhanden ist. Daher geben moderne E-Learnings den Lernenden nicht nur die Möglichkeit, effektiv zu lernen, sondern versetzen ihn und sie in die Lage, das Wissen immer aufrufen zu können. Daher funktionieren moderne Trainings wie Nachschlagewerke. Ein Beispiel: Bei einer verdächtigen Mail, können die Lernenden das entsprechende Training direkt aufschlagen und gezielt nachschauen, ob gewisse Merkmale auf ihre aktuelle Situation zutrifft. So fließen Trainings im Optimalfall in den Arbeitsalltag ein und entwickeln somit einen maximalen Lerntransfer.

Kognitiv lässt sich der Vorgang folgendermaßen erklären: Lerner*innen haben das Wissen aus dem E-Learning immer noch parat und die Mail hat aus diesem Grund Misstrauen erweckt. Sie erinnern sich genau an die entsprechende E-Learning-Einheit, in welcher sehr greifbar, bildlich und nachhaltig erklärt wird, woran verdächtige Mails erkennbar sind. Die moderne Lernmethode hat so geholfen, einen echten Angriff zu erkennen und damit richtig umzugehen. So verknüpfen die Lerner Trainings und Arbeitsallag. „Workplace Learning“ findet in solchen Fällen statt, was wiederum dazu führt, dass der Lerner Inhalte bzw. Wissen am effektivsten verinnerlicht.

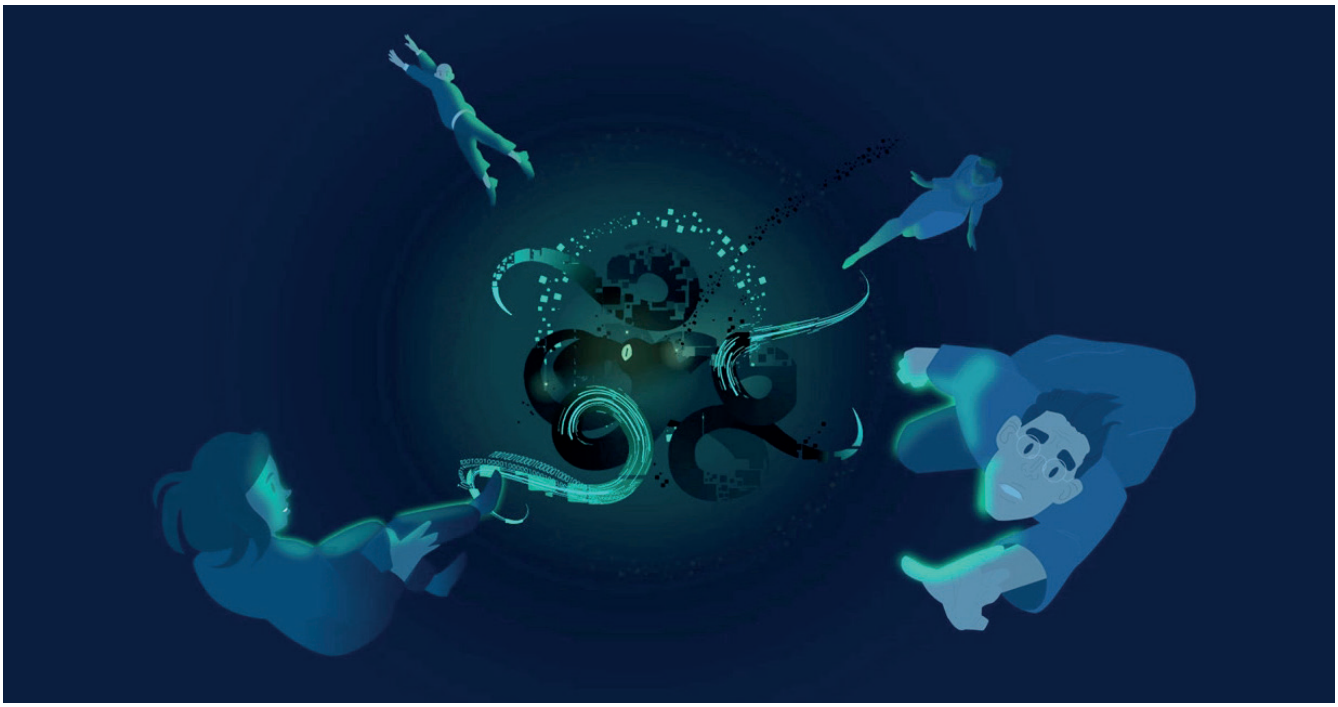
WARUM STORYTELLING DEN LERNERFOLG VERBESSERT

Schon aus der Schulzeit wissen wir, dass jeder Mensch unterschiedlich lernt. Die eine lernt immer noch gerne klassisch mit viel Text und Zahlen, der andere lieber explorativer, also im Zuge einer Geschichte, die einem rund um ein Thema erzählt wird. Am Ende lernt jede*r auf eine eigene Weise – es gibt keinen richtigen oder falschen Ansatz. Jede Methode, die einem Menschen hilft, Sachen zu lernen, ist für den Einzelnen die richtige.

Allerdings zeigt sich, dass eine Mehrheit zum zweiten Lernansatz tendiert. Insbesondere junge Menschen lernen eher explorativer, weil sie im Alltag von Stories und einer storygetriebenen Erzählweise in Social Media wie Instagram, bei Serien von Streaming-Portalen und auch Computerspielen umgeben sind. Wir konsumieren Geschichten als Filme, Serien, Bücher, Comics oder erzählen sie uns gegenseitig. Unser Leben ist eine einzige Ansammlung von Geschichten. Ein großer Teil dieser Stories gibt bewusst oder unbewusst Wissen weiter. Der Vorteil von geschichts- bzw. storygetriebenen Elementen wird vor allem im Bereich der E-Learnings deutlich.

Daher folgen viele E-Learnings dem sogenannten Storytelling-Ansatz. Das Thema der Lerneinheit wird dabei mit einer passenden Geschichte verknüpft – natürlich fließen dabei alle wichtigen Zahlen, Daten und Fakten in die Geschichte mit ein. Im Zuge des Storytellings kommen meistens speziell dafür geschaffene Charaktere zum Einsatz, sodass die Lernenden nicht nur durch eine erzählte Geschichte lernen, sondern das Gelernte auch an Personen knüpfen können, die einem vertraut sind. Gewisse Erfahrungen und Begebenheiten behalten wir Menschen besser im Gedächtnis, wenn sie mit Personen und Umgebungen oder mit anderen Reizen (Gerüche etc.) verknüpft sind. Entscheidend ist: Unser Gehirn unterscheidet nicht, ob wir das selbst erleben oder ein Charakter. Deshalb speichern wir die Information auch so gut.

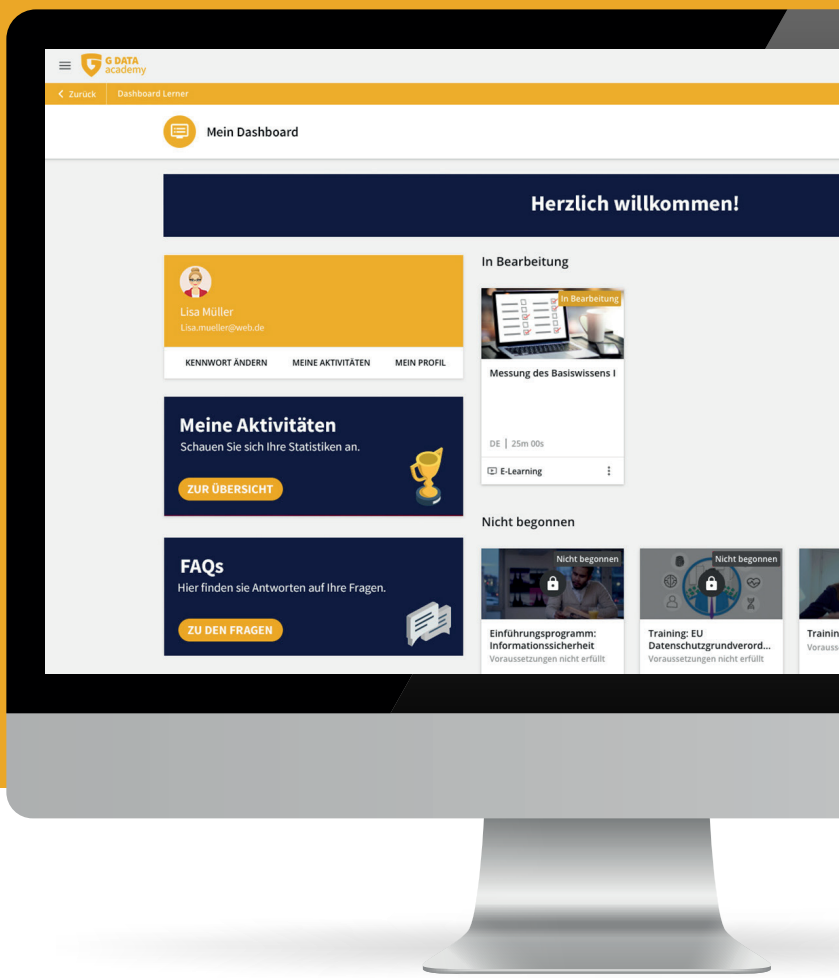
Bei allen Vorteilen von Storytelling gilt eine Regel ganz besonders: „In der Kürze liegt die Würze." Die beste Geschichte wird mit der Dauer langweilig, wenn sie in viel zu epischer Breite ausgerollt wird. Speziell bei E-Learnings gilt der Ansatz: Ein Themengebiet, zum Beispiel Phishing, wird einerseits in einer korrespondierenden Geschichte erzählt – mit entsprechenden Charakteren, andererseits braucht es mehrere Trainingsepisoden, um sämtliche Inhalte ausführlich zu behandeln. Denn Lerneinheiten, die länger als zehn Minuten sind, sorgen dafür, dass die Aufmerksamkeit ebenso wie der Spannungsbogen der Geschichte sinkt. Und damit auch der Lerneffekt.



G DATA academy

Sind Sie neugierig geworden?
Probieren Sie unsere Trainings gerne selbst aus und sehen Sie, wie wir Stories und spielerische Ansätze in unseren Lerninhalten einsetzen.

Hier geht es zur Testversion:
gdata.de/awareness-training



WAS UNSERE KUNDEN SAGEN

„Die Security Awareness Trainings von G DATA sind didaktisch sehr gut aufgebaut und decken das Thema umfassend ab. Das Lernen der komplexen Materie macht Spass und die interaktiven Elemente binden die Lerner*innen ein, sodass sie die Kurse bis zum Ende absolvieren."

Sandra Käppeli
Area Managerin ICT bei der Streamline AG