axians

Coachen Sie Ihre Human Firewall

Mit Security Awareness Training zu mehr Sicherheits- und Risikobewusstsein im Unternehmen

VINCI ENERGIES

Inhalt

Unternehmen haben unter den Angriffen erheblich zu leiden. Längst hat der wirtschaftliche Schaden – mit mehreren Milliarden Euro jährlich – eine astronomische Größenordnung erreicht.

Dass Cyberangriffe sich zu einer solch immensen Bedrohung für Unternehmen entwickeln konnten hat nicht zuletzt eine Ursache: nach wie vor besteht bei der Belegschaft eine hohe Anfälligkeit für manipulative Ausspähversuche. Nur wenige – zu wenige – Mitarbeiter sind sich der Risiken des Cyberspace tatsächlich bewusst und in der Lage zu erkennen, wenn ein Unberechtigter versucht, an ihre Nutzerdaten zu gelangen. Mit technischen Sicherheitslösungen allein ist diesem Problem nicht beizukommen. Unternehmen müssen, wollen sie das Risiko ihrer Mitarbeiter, manipuliert und ausgespäht zu werden, reduzieren, deren Sicherheits- und Risikobewusstsein anheben. Sie benötigen ein wirkungsvolles und nachhaltiges Cyber Security Awareness Training.

Auch in Deutschland haben Unternehmen seit Jahren mit einem kontinuierlichen Anstieg der Cyberangriffe zu kämpfen. Diese können gravierende Schäden nach sich ziehen, wie:

Die teilweise Störung oder vollständige Unterbrechung der Betriebsabläufe

Die Entwendung von Betriebsgeheimnissen

Immense Imageschäden bei Partnern und Kunden

Kleine und mittlere Unternehmen sind hier schnell in ihrer Existenz bedroht. Auf mehrere dutzend Milliarden Euro jährlich werden die durch Cyberangriffe entstandenen Schäden mittlerweile geschätzt – allein im deutschen Wirtschaftsraum.

Der Mitarbeiter im Fokus von Kriminellen

Für gewöhnlich sind es die Mitarbeiter, welche von den Angreifern als erstes Ausspähziel ausgemacht werden. Nur die wenigsten von ihnen verfügen über ein ausgeprägtes Bewusstsein für die Risiken des Cyberspace. Noch weniger besitzen grundlegende Basiskenntnisse im Bereich der Cybersicherheit.
Diese Schwachstellen nutzen die Angreifer gezielt für sich aus. Unter Rückgriff auf Methoden der angewandten Sozialwissenschaft und unter Zuhilfenahme fingierter und präparierter E-Mails und Webseiten werden Mitarbeiter ausgespäht, analysiert und schließlich manipuliert, um sie zu einer Handlung zu bewegen an deren Ende der Kriminelle sich in den Besitz ihrer Zugangsdaten bringt. Diese werden dann von ihm genutzt, um in einem zweiten Schritt – unbemerkt von der Cyber Security – in das Unternehmensnetzwerk einzudringen, Malware zu installieren, Systemeinstellungen zu verändern oder Daten zu entwenden.
Will ein Unternehmen diese Schwachstelle effektiv ausmerzen, wird es das Sicherheits- und Risikobewusstsein seiner Mitarbeiter nachhaltig anheben müssen. Eine große Aufgabe, die eine umfassende Einbindung aller Interessenvertreter erforderlich macht.

Die Sicherheit der Mitarbeiter – eine Aufgabe für das ganze Unternehmen

Um effektiv gegen Cyberangriffe auf Mitarbeiter vorzugehen, bedarf es eines nachhaltigen Cyber Security Awareness Trainings für die gesamte Belegschaft. Damit dieses Training jedoch die gewünschten Erfolge zeitigen kann, müssen alle Interessenvertreter umfassend in dessen Konzeption und Umsetzung eingebunden werden:

- von der Unternehmensführung,
- über die IT-Sicherheitsabteilung,
- bis hin zu den Betriebs- und Personalräten.

Gerade Letztere werden meist außenvorgelassen, wenn es um die Cyber Security eines Unternehmens geht. Kommen beim Schutz der IT doch häufig allein technische Lösungen zum Tragen. Hier jedoch – wo es darum geht, die Belegschaft durch Schulungsprogramme zu stabilen Gliedern der unternehmensinternen Abwehrkette zu formen – ist solch ein Vorgehen kontraproduktiv. Gerade bei langandauernden Trainingsprogrammen ist es unabdingbar, Betriebs- und Personalräte umfassend miteinzubeziehen.

Denn nachhaltig müssen die Schwächen jedes einzelnen Mitarbeiters neutralisiert, die Stärken gefördert werden. Hier maximale Erfolge zu erzielen, verlangt, jede wohlüberlegte Sicherheitsentscheidung des Mitarbeiters zu fördern, gezielt Motivation für das richtige Sicherheitsverhalten zu schaffen.

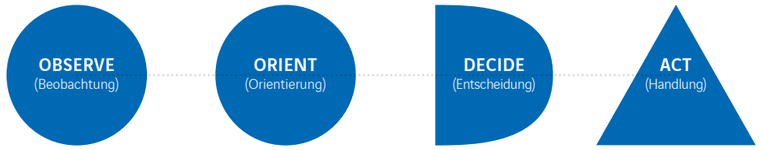
Eine effektive Einbindung der Betriebs- und Personalräte ist hierbei unerlässlich. Andernfalls wird das Training unnötig auf eine reine, kurzfristige Wissensvermittlung reduziert. Den ausgereiften Angriffstechniken der Kriminellen, die nicht selten auf psychologischen Tricks basieren, ist so aber nicht beizukommen.

SOCIAL ENGINEERING

Das Opfer im Griff

Um bei den Mitarbeitern den gewünschten Erfolg zu erzielen, greifen Kriminelle bei ihren Ausspähversuchen für gewöhnlich auf Methoden der angewandten Sozialwissenschaften, auch bekannt als Social Engineering oder 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, werden ihnen falsche Informationen vorgespielt, werden sie so lange psychischem Druck ausgesetzt, bis sie endlich – quasi reflexhaft – in der gewünschten Art und Weise reagieren.

Der Angreifer nimmt dabei direkten Einfluss auf das Entscheidungsverhalten seiner Opfer. Wie ihm dies gelingt, veranschaulicht das Informationsstrategiemodells der sogenannten OODA-Schleife, des US-amerikanischen Militärstrategen James Boyd. OODA setzt sich zusammen aus:



Laut Boyds Modell stellen diese vier Handlungen – in direkter Aufeinanderfolge – einen typischen Entscheidungsprozess dar. Ein Angreifer kann den Entscheidungsprozess seines Opfers nun in eine für diesen ungünstige Richtung lenken. Hierzu muss er diesen lediglich täuschen oder vieldeutigen Ereignissen aussetzen. Der Social Engineer streut hierzu Falschinformationen, spielt Wissen und Autorität vor und drängt sein Opfer zu unverzüglichem Handeln. So gelingt es ihm, den vierteiligen Entscheidungsprozess auf die beiden letzten Bestandteile Entscheidung und Handlung zu verkürzen und sein Opfer vollends unter Kontrolle zu bekommen.

Die wohl populärste Social Engineering-Angriffstechnik – und derzeit am häufigsten gebrauchte Variante von Cyberangriffen auf Unternehmen – stellt das Phishing dar.

PHISHING-ANGRIFFE

Nichts ahnend wird das Mitarbeiterkonto zum Einfallstor

Bei einem Phishing-Angriff werden die Opfer über gefälschte E-Mails, Webseiten oder SMS dazu verleitet, vertrauliche Informationen, wie zum Beispiel ihren Benutzernamen und ihr Passwort, weiterzugeben. Hat der Kriminelle diese Daten erbeutet, loggt er sich, unter dem Account seines Opfers, in das Netzwerk seines eigentlichen Ziels ein. Nun kann er – unbemerkt von deren Cyber Security – deren IT-Infrastruktur durchstöbern, analysieren und für den eigentlichen Angriff präparieren.

91 Prozent aller derzeit auf ein Unternehmen gerichteten Ausspähmaßnahmen basieren letztlich auf solchen Phishing-Attacken.

Will ein Unternehmen sich hiergegen schützen, will es das Risiko seiner Mitarbeiter, Opfer eines solchen Ausspähversuchs zu werden, minimieren, kommt es um eine Schulung des Sicherheitsbewusstseins seiner Mitarbeiter nicht herum. Sie müssen lernen, im entscheidenden Moment richtig zu handeln und auch unter Druck stets die Kontrolle über ihre Entscheidungen zu behalten.

Die eigenen Mitarbeiter als „Human Firewall“

Bereits heute stellen Mitarbeiter regelmäßig unter Beweis, dass sie durchaus in der Lage sind, einen Beitrag zur Cyber Security ihres Unternehmens zu leisten. **In einer 2018 veröffentlichen Studie des Digitalverbandes Bitkom gaben 61 Prozent der befragten deutschen Industrieunternehmen zu Protokoll, schon mindestens einmal durch direkte Hinweise ihrer Mitarbeiter auf einen Cyberangriff aufmerksam gemacht worden zu sein.** Die Zahl verdeutlicht das Potential, das im Einsatz von Mitarbeitern im Sicherheitsbereich schlummert.

Denn bislang haben Unternehmen nur wenig – zu wenig – unternommen, dieses Potential zu heben und voll zu entfalten. Nach wie vor ist die Mehrzahl der Mitarbeiter nicht in der Lage, sich bewusst sicher im Cyberspace zu bewegen. Verdächtig anmutende Dateien oder Aufforderungen erscheinen ihnen nicht suspekt. Sie wissen nicht, welche ihrer Handlungen im Cyberspace von Kriminellen für deren Machenschaften ausgenutzt werden können und welche nicht.
Sie benötigen ein effektives Cyber Security Awareness Training, das nachhaltig die gesamte Belegschaft zu einer festen Größe der Cyber Security macht.

Reguläre Security Awareness Trainings nicht nachhaltig genug

Einfache Trainings zur Anhebung des Sicherheitsbewusstseins der Mitarbeiter, sogenannte Cyber Security Awareness Trainings, sind schon länger auf dem Markt erhältlich und werden von Unternehmen auch gut frequentiert. Doch weisen sie für gewöhnlich drei Schwachstellen auf:

- Passivität der Lernmethoden,
- Inflexibilität der Lerninhalte und
- Überkomprimierung der Lehrzeit.

Für gewöhnlich besteht das Training aus einfachem Frontalunterricht. Die Mitarbeiter hören nur passiv zu und werden – abgesehen von gelegentlichen Tests – nicht wirklich aktiv beansprucht. Darüber hinaus sind die Trainingsprogramme meist so angelegt, dass jedem Mitarbeiter dieselben Inhalte präsentiert werden. Auf unterschiedliche Funktionen und Sicherheitsanforderungen oder Präferenzen bei den Lerntypen wird keine Rücksicht genommen. Und schließlich ist der zeitliche Rahmen meist zu kurz bemessen, wird das Training in ein oder zwei komprimierten Blöcken absolviert. All dies trägt nicht dazu bei, dass Mitarbeiter die ihnen vermittelten Inhalte nachhaltig erfassen können.
Hinzu kommt, dass es Unternehmen für gewöhnlich an einer Möglichkeit fehlt, den Erfolg des Trainings objektiv festzustellen.

Der kann – im Fall der regulären Trainings – durchaus bezweifelt werden. Eine wissenschaftliche Untersuchung zum Sicherheitsverhalten von auf diesem Wege geschulten Offiziersanwärtern der US-Militärakademie West Point führte 2004 Erschreckendes zu Tage: **Wurden die Offiziersanwärter nach ihrer Sicherheitsschulung mit Social Engineering Methoden attackiert, fielen auch jetzt noch über 90 Prozent von ihnen darauf herein.**

In vielen Unternehmen wurden die Investitionen in Cyber Security Awareness Trainings in den letzten Jahren deshalb wieder zurückgefahren. Dabei kann ein Cyber Security Awareness Training – richtig angelegt – durchaus erfolgreich sein und das Sicherheitsrisiko eines Unternehmens nachhaltig senken.

Das nachhaltige Security Awareness Training

Wie solch ein nachhaltiges Security Awareness Training aussehen kann zeigt unser Partner KnowBe4. Statt allein auf ein einfaches Training, setzt es auf einen Dreiklang aus sich ständig wiederholenden Trainings-, Test- und Analyseeinheiten. Der Mitarbeiter durchläuft einen stetigen Kreislauf, an dem sein Sicherheits- und Risikobewusstsein langsam und nachhaltig wächst. Das Training:

- **bindet die Mitarbeiter aktiv in die Lernprozesse ein,**
- **ist zugeschnitten auf die Kultur der Organisation und die Funktionen, Sicherheitsfreigaben, Stärken, Schwächen und Lerntyppräferenzen der Mitarbeiter und**
- **ist portioniert in Themenblöcke, die in regelmäßigen Abständen über längere Zeiträume vermittelt werden.**

Im Ergebnis sorgt diese Vorgehensweise für einen deutlich höheren Lern- und länger anhaltenden Anwendungserfolg.

Security Awareness Training

Begleitet werden diese Trainingseinheiten von regelmäßigen Tests, den sogenannten Phishing-Simulationen. Hierbei werden Mitarbeiter in ihrem regulären Arbeitsalltag mit verdächtigen Daten und Aktivitäten – welche sie in den Trainingsphasen bereits kennengelernt haben – konfrontiert und dahingehend überprüft, ob sie diese nun auch tatsächlich wiedererkennen, meiden und melden.

Anschließend werden die Ergebnisse dieser Tests, unter Wahrung der Vorgaben des Bundesdatenschutzgesetzes (BDSG) und der EU-Datenschutzgrundverordnung (EU-DSGVO), ausgewertet und analysiert. Erstmalig kann ein Unternehmen so ermitteln, ob und wie das Training bei den Mitarbeitern tatsächlich anschlägt, welche Mitarbeiter anschließend bewusster Risiken in Cyberspace wahrnehmen und bei welchen weitere Trainingseinheiten erforderlich sind.
Wichtiger noch, erstmalig erhalten Mitarbeiter so ein Training, dessen Inhalte – durch ständige Repetition – tief in ihrem Bewusstsein verankert werden. Das Risiko, Opfer einer Social Engineering-Attacke zu werden, kann so deutlich gesenkt werden.

Geschützt gegen Social Engineering-Ausspähmaßnahmen

Denn durch Phishing-Simulationen und ein individualisiertes kontinuierliches Training über längere Zeiträume bleibt der Trainingserfolg nicht allein auf einen simplen Wissensgewinn begrenzt. Vielmehr werden nachhaltige Änderungen im Sicherheit- und Risikoverhalten provoziert.

Um sich effektiv vor den Social Engineering-Methoden der Kriminellen zu schützen, müssen Mitarbeiter in die Lage versetzt werden, diese innerhalb von Sekunden – quasi automatisch – zu durchschauen. Sie müssen, ohne nachzudenken – unterbewusst – richtig handeln.

Dies gelingt nur mit einem kontinuierlichen, interaktiven Training. **66 Tage ständiger Wiederholung, dies ergab eine Studie von Verhaltensforschern des Londoner University College, benötigt das menschliche Gehirn im Schnitt, um eine Handlung in seine Alltagsroutine zu integrieren.** Nur bei ausreichender Dauerbelastung, bei kontinuierlichem Training und regelmäßigen Phishing-Simulationen, gräbt sich das Wissen um die Risiken des Cyberspace tief ins Bewusstsein der Mitarbeiter ein; bis es zu einem Reflex wird, der in verdächtigen Situationen automatisch anschlägt. Social Engineering-Attacken haben dann keine Chance mehr.

Die vier Kompetenzstufen

Quelle: Nœl Burch, Gordon Training international, Consious Competence Ladder

Photo by Thao Le Hoang on Unsplash

Fazit

Anders als reguläre Sicherheitstrainings setzt das Security Awareness Training von KnowBe4 auf eine Serie von Schulungen, Tests im Arbeitsalltag und quanti- wie qualitativen Analysen, um das Sicherheits- und Risikobewusstsein der Mitarbeiter eines Unternehmens nachhaltig anzuheben.
Dass das neue Trainingskonzept sich im Alltag auch tatsächlich bewährt, hat unser Partner bereits im vergangenen Jahr in einer Studie unter Beweis stellen können. In dieser ein Jahr dauernden Untersuchung wurden 6 Millionen Nutzer seines Security Awareness Trainings im Hinblick auf dessen Auswirkungen auf ihr Sicherheits- und Risikoverhalten analysiert. Das Ergebnis spricht für sich.

Quelle: KnowBe4

27 Prozent der Nutzer führten zu Beginn des Trainings unbewusst gefährdende Handlungen aus, die von einem Angreifer für einen Phishing-Angriff hätten genutzt werden können. Bereits nach 3 Monaten war diese Zahl auf 13 Prozent gefallen. Nach einem Jahr kontinuierlichen Trainings konnten dann nur noch 2,2 Prozent der Nutzer gefährdende Handlungen nachgewiesen werden. Die Studie zeigt: **mit dem richtigen Trainingskonzept können Unternehmen sehr wohl weitreichende, langanhaltende Erfolge bei der Senkung ihrer Sicherheitsrisiken erzielen.**

Es besteht also kein Grund, die Mitarbeiter allein als Belastung der Cyber Security zu begreifen. Sie können sehr wohl einen realen sicherheitspolitischen Mehrwert besitzen. Die Interessenvertreter der Unternehmen müssen diesen nur erkennen, heben und gemeinsam fördern. Eine entscheidende Rolle kommt hierbei den Betriebs- und Personalräten zu. Kann ihre umfassende Einbindung die Effektivität des Trainingsprogramms doch noch einmal bedeutend erhöhen. Sind die Mitarbeiter dann erst einmal mit dem notwendigen Sicherheits- und Risikobewusstsein ausgestattet, ist die „Human Firewall" erfolgreich installiert und das Unternehmensrisiko, Opfer eines Cyberangriffs zu werden, nachhaltig reduziert.

In Zusammenarbeit mit
unserem renommierten Partner

KnowBe4
Human error. Conquered.

08/2020

axians

Axians IT Security GmbH · Arndtstraße 25 · 22085 Hamburg
Tel.: +49 40 271661-0 · Fax: +49 40 271661-44
E-Mail: info-itsecurity@axians.de · www.axians.de