Awareness top-down verankern

Know-how In rund 80 Prozent der Cybervorfälle ist der Mensch der Ausgangspunkt. Phishing-Mails, täuschend echte Nachrichten und SMS-Angriffe mit abgegriffenen MFA-Codes reichen oft für den ersten Zugriff. Ein aktueller Fall mit Millionenschaden zeigt das deutlich.

Von Jill Wick

Ein erfolgreicher CEO-Fraud kostete ein Unternehmen im Kanton Schwyz mehrere Millionen Franken. Der Cybervorfall sorgte landesweit für Schlagzeilen und führt exemplarisch vor Augen, wie schnell Handeln unter Druck zur Einflugschneise moderner Social-Engineering-Angriffe wird. Kurzum: Wo eine gelebte Awareness-Kultur fehlt, können kritische Situationen schnell zu Schäden in Millionenhöhe eskalieren.

Wissensdefizit oder organisatorischer Mangel?

Die öffentliche Debatte rund um den Vorfall zeigt exemplarisch, wie Security Awareness nach wie vor wahrgenommen wird. In Medienkommentaren und Leserreaktionen wird Verantwortung auf Einzelpersonen verschoben, Entwicklungen technologisch erklärt oder verpflichtende Schulungen gefordert. Was auffällt: Kaum jemand fragt nach der organisatorischen Verantwortung hinter solchen Vorfällen.

Gerade darin liegt die Aussagekraft der öffentlichen Kommentierung: Sie bündelt nahezu das gesamte Spektrum der Fehlwahrnehmungen, mit welchen CIOs und CISOs heute konfrontiert sind. Insbesondere der Ruf nach «verpflichtenden Schulungen» greift zu kurz, solange Awareness als reiner Lerninhalt und nicht als Gesamtsystem für kulturellen Wandel verstanden wird. Damit verschiebt diese Sichtweise die Verantwortung fälschlicherweise auf die Mitarbeitenden.

Die regulatorische Realität

Die Geschäftsleitung verantwortet die wirksame Umsetzung und Einhaltung gesetzlicher Sicherheitsvorgaben. Das revidierte Datenschutzgesetz sowie weitere branchenspezifische Regelwerke verorten die Sicherstellung der Cyberresilienz klar auf Managementebene.

Die Realität spiegelt jedoch eine andere Wahrnehmung. In vielen Unternehmen hält sich die Annahme, eine einmalige Awareness-Schulung reiche aus, um Mitarbeitende dauerhaft für die zentralen Risiken zu sensibilisieren. Solche Trainings erzeugen in der Praxis lediglich ein formales Sicherheitsgefühl, ohne substanzielle Sicherheit zu schaffen. Tritt dennoch ein Cybervorfall ein, rechtfertigen sich Organisationen nicht selten damit, dass die Mitarbeitenden doch informiert gewesen seien und eine obligatorische Schulung absolviert hätten. Diese Sichtweise verkennt den eigentlichen Kern des Problems. Awareness ist eine strategische Governance-Aufgabe, die psychologische Sicherheit schafft und organisationale Cyberresilienz ermöglicht.

Klickraten statt Handlungsfähigkeit

Klassische Awareness-Ansätze reduzieren Security Awareness noch heute vielfach auf messbare Kennzahlen wie Klickquoten bei Phishing-Simulationen oder Abschlussraten von E-Learnings. Diese Ergebnisse belegen zwar ein gewisses Risikobewusstsein bei Mitarbeitenden, nicht jedoch, dass daraus wirksame Sicherheitsprozesse abgeleitet wurden. Offen bleibt zudem, ob klare Handlungsanweisungen existieren, die Mitarbeitenden befähigen, Sicherheitsvorfälle zu erkennen, einzuordnen und im Ernstfall angemessen zu handeln. Hier offenbart sich ein fundamentales Spannungsfeld: Awareness-Ziele orientieren sich häufig an tatsächlicher Handlungsfähigkeit. Entscheidend ist nicht, dass «80 Prozent ein E-Learning abgeschlossen haben», sondern dass Mitarbeitende im Ernstfall wissen, an wen sie sich wenden können und wie sie richtig handeln.

Die Verankerung in NIS2, revDSG und FINMA

Security Awareness ist längst mehr als nur eine regulatorische Vorgabe – sie ist verpflichtend. In Regelwerken wie dem revidierten Schweizer Datenschutzgesetz (revDSG), dem FINMA-Rundschreiben oder der europäischen NIS2-Richtlinie wird Cybersicherheit ausdrücklich auf Managementebene adressiert, einschliesslich der Verantwortung für Lieferketten. Damit konkretisiert sich die Sorgfaltspflicht: Die Geschäftsleitung verantwortet den Aufbau und die Wirksamkeit eines belastbaren, resilienten Awareness-Konzepts. Verstösse können persönliche Haftungsrisiken nach sich ziehen.

In der Praxis bleibt diese regulatorische Verankerung jedoch oft unvollständig. Viele Organisationen statten Security Awareness nur zögerlich mit Ressourcen aus und überlassen es einzelnen Verantwortlichen, ihre strategische Relevanz intern zu legitimieren. Solange Awareness als reines «Wissensthema» und nicht als Bestandteil der Unternehmensstrategie verstanden wird, entstehen gefährliche Abstimmungslücken mit realem Risiko.

Awareness ohne Awareness-Kultur

Ein Blick in die Praxis zeigt, wie Awareness ohne organisatorische Verankerung

ins Leere läuft. Eine Fachabteilung entscheidet eigenständig für die Einführung eines Passwortmanagers. Grundsätzlich ist dies ein sinnvoller Schritt, der Effizienz und Cyberresilienz steigern kann. Die Sicherheitsabteilung jedoch bleibt aussen vor und hat weder Gelegenheit, die Lösung vorab zu prüfen, noch sie in bestehende Sicherheitsprozesse einzuordnen.

In der Folge beauftragt die Organisation das Awareness-Team, ein E-Learning zu entwickeln, das die Belegschaft zur Nutzung des Passwortmanagers anleiten soll. Awareness wird damit zur nachgelagerten Korrektur eines bereits getroffenen Entscheids, organisatorisch entkoppelt und ohne strategische Einbettung. Somit fehlt eine übergeordnete Governance, die Sicherheit, IT und Awareness von Beginn an zusammenführt. Ohne ein solches Fundament verfestigen sich isolierte Einzelmassnahmen statt wirksamer Sicherheitsstrukturen.

Nachhaltige Handlungsfähigkeit statt Silo-Entscheidungen

Silo-Entscheidungen verweisen auf ein strukturelles Defizit. Wird Awareness auf die nachträgliche Korrektur strategischer Versäumnisse reduziert, fehlt die Grundlage für einen nachhaltigen Aufbau von Cyberresilienz.

Ein fehlendes oder unzureichend verankertes Awareness-Konzept weist deshalb nicht auf ein Defizit der Mitarbeitenden hin, sondern auf einen übergeordneten Mangel auf Organisationsebene. Wirksam gegensteuern lässt sich nur mit einer verbindlichen Governance, welche Technik, Prozesse und menschliche Handlungsfähigkeit von Beginn an miteinander verzahnt und von einem strategisch etablierten Awareness-Konzept getragen ist.

Was «gute» Security Awareness wirklich leistet

Ziel ist nicht, Mitarbeitende zu fehlerfreien Sicherheitsexperten auszubilden. Entscheidend ist vielmehr, Organisationen so aufzustellen, dass Fehler früh erkannt, korrekt bewertet und sicher eskaliert werden. Diese Transformation kann nur gelingen, wo Security Awareness systematisch verankert ist. Voraussetzung dafür sind klare Prozesse, eindeutig geregelte Verantwortlichkeiten und die Einbettung in die Unternehmensstrategie.

In der Praxis bedeutet dies, Security Awareness nicht isoliert zu betrachten, sondern eng in die operativen Sicherheitsstrukturen zu integrieren. Beispiele hierfür sind das Security Operations Center (SOC), die Incident Response und regelmässige Krisenübungen. Wo interne Ressourcen an Grenzen stossen, ergänzen spezialisierte externe Partner diese Strukturen gezielt. So bleibt Handlungsfähigkeit im Ernstfall gewährleistet und Mitarbeitende wissen, was zu tun ist.

Awareness entsteht im operativen Alltag

Wirksame Awareness-Arbeit orientiert sich somit am operativen Alltag und richtet sich an den konkreten Anforderungen der jeweiligen Branchen aus. Besonders bewähren sich Szenarien aus dem eigenen Betrieb, die reale Abläufe und konkrete Entscheidungssituationen abbilden.

So trainieren etwa Kliniken den Umgang mit Anfragen von Angehörigen und den Schutz sensibler Patientendaten. Banken wiederum schärfen den Blick für die Klassifizierung von Informationen sowie den Schutz kritischer Finanz- und Zahlungsdaten. Awareness entfaltet ihre Wirkung dort, wo Entscheidungen tatsächlich getroffen werden: im operativen Alltag.

Wiederholung, Orientierung und Feedback

Erkenntnisse aus Werbung und Pädagogik zeigen: Ein einmaliger Impuls reicht nicht aus, um Verhalten nachhaltig zu verändern. Entscheidend ist, dass Mitarbeitende wissen, wo sie verlässliche Informationen finden und an wen sie sich im Zweifelsfall wenden können. Ihre volle Wirkung entfaltet Awareness als kontinuierliche Präsenz im Alltag: mit wiederholten Kernbotschaften, klar definierten Eskalationswegen und zeitnahen, konkreten Rückmeldungen auf Anfragen und Hinweise.

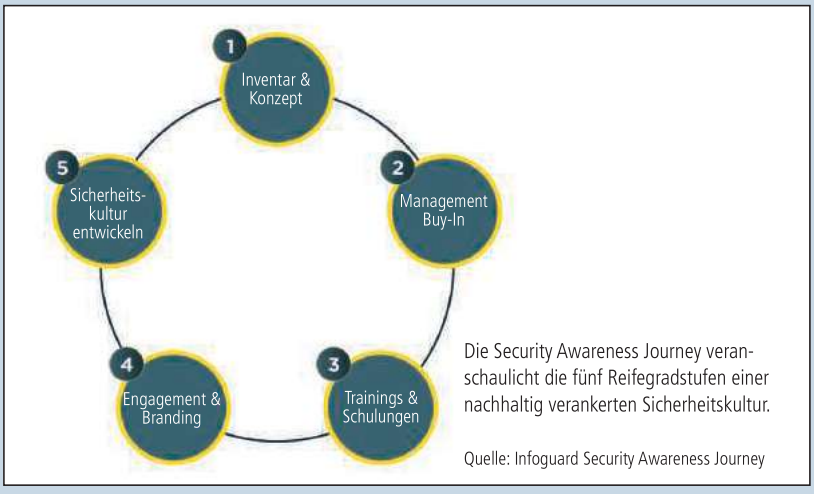
Fehlende oder abwertende Rückmeldepraxis sowie die Sanktionierung kritischer Fragen schwächen nachhaltig die Bereitschaft, Bedrohungen und Risiken zu melden. Ein zentrales Prinzip entscheidet in all diesen Situationen über Wirksamkeit: psychologische Sicherheit.

Psychologische Sicherheit als fester Teil der Firmenkultur

Psychologische Sicherheit entsteht dort, wo Führung offenes Ansprechen aktiv fördert, Rückfragen ausdrücklich zulässt und Fehler nicht sanktioniert. Mitarbeitende sollen Probleme und Zweifel offen ansprechen und auch unbequeme oder vermeintlich naive Fragen stellen dürfen,

SICHERHEITSKULTUR IN FÜNF ETAPPEN ETABLIEREN

Nachhaltige Cyberresilienz entsteht nicht durch einmalige Schulungen, sondern durch eine systematische Verankerung im Unternehmen. Die Security Awareness Journey strukturiert diesen Prozess in fünf Reifegradstufen – von der Entwicklung eines fundierten Konzepts über das Management Buy-in und zielgerichtete Schulungen bis hin zu aktivem Mitarbeitenden-Engagement und einer gelebten Sicherheitskultur. Organisationen können, abhängig von ihrem aktuellen Reifegrad, gezielt einsteigen und den nächsten Entwicklungsschritt systematisch erreichen.



Die Security Awareness Journey veranschaulicht die fünf Reifegradstufen einer nachhaltig verankerten Sicherheitskultur.

Quelle: Infoguard Security Awareness Journey

ohne negative Konsequenzen befürchten zu müssen.

Erst diese Handlungssicherheit schafft die psychologische Grundlage, Risiken frühzeitig zu benennen und im Ernstfall zu handeln. Sie wird jedoch erst wirksam, wenn Organisationen diese psychologische Sicherheit fest in ihre Prozesse und Arbeitsabläufe integrieren. Nicht als begleitende Initiative, sondern als fester Bestandteil des operativen Alltags.

Was Organisationen von KI-Assistenten lernen können

KI-Assistenten veranschaulichen dieses Prinzip besonders deutlich. Sie reagieren auf Fragen grundsätzlich wertschätzend, signalisieren Offenheit und verfolgen einen klar lösungsorientierten Ansatz.

Diese Form der Interaktion senkt Hemmschwellen: Wer sich ernst genommen fühlt, fragt nach, äussert Unsicherheiten und benennt Fehler früher. Genau hier liegt der übertragbare Kern. Übernehmen Führungskräfte diese Haltung im Umgang mit Mitarbeitenden, entsteht ein Arbeitsumfeld, das Offenheit systematisch begünstigt. Damit gilt: Wo Fragen nicht als Störung wahrgenommen und Zweifel frühzeitig addressiert werden, entsteht ein substanzieller Beitrag zur Cybersicherheit eines Unternehmens.

Wenn Schweigen Cybervorfälle begünstigt

Sprechen Mitarbeitende Fehler offen an, lassen sie sich einordnen, besprechen und korrigieren. Verschweigen sie hingegen Handlungsfehler, können diese schwerwiegende Konsequenzen nach sich ziehen. Das folgende Beispiel verdeutlicht dies eindrücklich: Ein Mitarbeitender klickt auf ein täuschend echt gestaltetes Phishing-Mail. Kurz darauf öffnet sich ein Downloadfenster, das im nächsten Moment wieder verschwindet. Zurück bleibt ein vager Zweifel.

Mangels klarer Prozesse und fehlender psychologischer Sicherheit entscheidet sich der Mitarbeitende gegen eine Meldung des Vorfalls. Wochen später aktiviert sich eine Erpressungssoftware, die an jenem Tag unbemerkt den ersten Rechner infiziert hatte. Hätte die Organisation eine frühzeitige Meldung ermöglicht und eingefordert, hätte sie den Angriff isolieren und womöglich verhindern können.

Psychologische Sicherheit als Voraussetzung für Lernfähigkeit

Fehlt psychologische Sicherheit, ziehen sich Menschen zurück: Sie verschweigen Fehler, meiden Konflikte und hinterfragen bestehende Abläufe nicht mehr. Wo Organisationen hingegen psychologische Sicherheit aktiv fördern, entstehen offene Dialoge, konstruktives Feedback und die Bereitschaft, auch unbequeme Tatsachen auszusprechen.

Psychologische Sicherheit entsteht nicht punktuell. Sie entwickelt sich, wenn Führung sie sichtbar vorlebt und die Organisation sie systematisch in Strukturen, Prozesse und Kultur integriert.

Awareness-Kultur macht den Unterschied

Betrachten wir eine Organisation, die diese Prinzipien konsequent lebt. Wie würde sich das eingangs beschriebene Angriffsszenario in einem Unternehmen auswirken, das Awareness-Kultur bereits etabliert hat? Der Inhaber wird beim Lesen der Mails stutzig, bleibt vom Zeitdruck unberührt und prüft die ungewöhnliche Anfrage über einen zweiten, gesicherten Kommunikationskanal. In seinem Unternehmen gilt der Grundsatz «Sicherheit vor Geschwindigkeit», sichtbar durch die Führung vorgelebt.

Die Folge: Die Bedrohung wird erkannt und der Angriff scheitert. Innerhalb weniger Minuten informiert der Inhaber das Security-Team seiner Organisation, welches wiederum die Belegschaft vor dem laufenden Angriffsvektor warnt. Der Vorfall wird nicht verdrängt, sondern genutzt: Die Organisation übersetzt den Angriffsversuch in eine konkrete Sensibilisierung des gesamten Unternehmens, getragen und vorgelebt durch die Geschäftsleitung.

Strategisch verankerte Awareness schafft damit nicht nur Schutz, sondern auch Klarheit über Verantwortlichkeiten, Entscheidungswege und wirksames Handeln im Ernstfall. ■

DIE AUTORIN

Jill Wick ist Cyber Security Awareness Consultant bei Infoguard und Wirtschaftspsychologin MSc FH. Als Voice on Human Centred Security beschäftigt sie sich mit der Schnittstelle von Psychologie, Cybersicherheit und Technologie – insbesondere mit deren Auswirkungen auf den Menschen.