Security Awareness – ein wesentlicher Beitrag zur Unternehmenssicherheit

Spionage, Diebstahl und Datenverlust bedrohen in der heutigen vernetzten Welt vertrauliche Geschäftsdaten und das Know-how von Unternehmen. In den letzten Jahren wurde deshalb viel Geld in Hardware, Software und Sicherheitskonzepte investiert. Doch genügen diese Massnahmen, damit Sicherheit auch gelebt wird? Thomas Manser, René Stock

Die meisten Unternehmen haben in den letzten Jahren auf die ständig wachsenden Bedrohungen reagiert und ein Sicherheitsdispositiv aufgebaut. Sie haben in Sicherheitsinfrastruktur (Netzwerk, Firewall, Malware-Programme und dergleichen) investiert, Sicherheitsbeauftragte benannt und Sicherheitsrichtlinien für Mitarbeitende, Partner und Lieferanten formuliert. Damit ist ein gutes Fundament gelegt. Doch werden diese Massnahmen auch wirklich gelebt? Weiss jeder Mitarbeiter, dass er einen wesentlichen Beitrag zur Unternehmenssicherheit leistet? Hat ihn das Unternehmen auch dazu befähigt und motiviert?

Die Förderung von Sicherheitsbewusstsein (oder Security Awareness) ist keine einmalige Angelegenheit. Einzelmassnahmen verpuffen und geraten in Vergessenheit. Es braucht eine Security-Awareness-Kampagne mit mehreren aufeinander abgestimmten Elementen, um eine dauerhafte Veränderung des Sicherheitsbewusstseins herbeizuführen. Mögliche Elemente einer solchen Kampagne sind in der nebenstehenden Tabelle aufgeführt.

ELEMENT	BESCHREIBUNG	NUTZEN	PERIODIZITÄT
Einführungstag	Der Sicherheitsbeauftragte stellt im Rahmen des Einführungstages für neue Mitarbeitende Informationssicherheit vor.	Einstieg in Sicherheit, erste Informationen	monatlich, quartalsweise
Faltblatt	Jedem Mitarbeitenden wird ein Faltblatt mit den wichtigsten Sicherheitsvorschriften abgegeben.	Nachschlagewerk für die tägliche Arbeit	einmalig, bei Anstellung
Plakate	Originell gestaltete Plakate an wichtigen Standorten (Eingang, Lift, Caféteria) wecken die Aufmerksamkeit mit Bild und einfachen, originellen Botschaften.	Sicherheit wird zum Gespräch	1 Plakat pro Monat, verteilt über 4-8 Monate
Intranet	Informationen zu aktuellen Bedrohungen, Plakaten, Sicherheitsvorschriften usw. werden im Intranet publiziert.	Nachschlagewerk, Informationsbeschaffung, Know-how-Vermittlung	laufend
Sitzungen	Der Sicherheitsbeauftragte erhält bei Management-Sitzungen und Internanlässen z.B. 10 Minuten für ein aktuelles Sicherheitsthema.	Teaser, Sicherheit bleibt als wichtiges Thema auf der Agenda	quartalsweise
Sicherheitstag	In einem halben Tag werden aktuelle Sicherheitsthemen – mit aktiver Teilnahme der Teilnehmenden – geschult (Hands-on). Mit Vorteil werden externe Spezialisten und/oder Lieferanten beigezogen. Dieser Anlass kann auch mit Themen wie Brandschutz und Erster Hilfe kombiniert werden.	Praxisnahe Know-how-Vermittlung, Identifikation mit Sicherheit	halbjährlich, jährlich
E-Learning	Themen wie Informations- und Datenschutz sind als E-Learning-Inhalte auf dem Markt verfügbar. Mieten oder kaufen Sie diese Inhalte, ergänzen Sie diese mit ihren unternehmensspezifischen Richtlinien und motivieren Sie alle Mitarbeitenden, diesen Lerninhalt mit Abschlusstest zu absolvieren.	Know-how-Vermittlung und -Vertiefung	einmalig für alle bestehenden und für neue Mitarbeitende
Brown Bag	Vorträge über Mittag mit externen Referenten zu aktuellen Sicherheitsthemen geben Impulse und regen zu Diskussionen an.	Impulse und Denkanstösse, Aussensicht	quartalsweise, halbjährlich
Pen-Test	Externe Spezialisten führen Penetrationstests Ihrer Infrastruktur durch (z.B. ist Ihr Webshop sicher?), prüfen, ob Ihr Standardarbeitsplatz gefährdet ist, und versuchen, mit Social Engineering an vertrauliche Informationen Ihres Unternehmens zu gelangen.	Feststellen der Wirksamkeit der getroffenen Sicherheitsmassnahmen und der erreichten Security Awareness	jährlich, zweijährlich

Tabelle: Netzmedien AG

Kritische Erfolgsfaktoren

Beachten Sie bei der Umsetzung Ihrer Security-Awareness-Kampagne die folgenden Erfolgsfaktoren:

- Binden Sie einen einflussreichen Vertreter des Managements mit ein. So erhalten Sie nicht nur das Commitment des Managements, sondern auch dessen Sicht und Werte sowie einen wertvollen Kommunikationskanal.
- Holen Sie sich eine erfahrene externe Beratung ins Team. Damit erhalten Sie eine externe, betriebsfremde (und nicht -blinde) und unabhängige Sicht und profitieren von Erfahrungen aus anderen Organisationen. Zudem erhöht dies in der Regel die Akzeptanz im Management.
- Haben Sie Geduld. Denken Sie daran, dass eine Veränderung im Unternehmen viel Zeit und Wiederholung («steter Tropfen ...») benötigt.
- Benennen Sie einen Mr. Security. Security Awareness ist permanentes, internes Marketing. Gewinnen Sie einen fähigen Mitarbeiter, der diese Aufgabe mit Begeisterung wahrnimmt.
- Etablieren Sie das Traktandum Sicherheit in Geschäftsleitungs- und Kadersitzungen sowie im Jahresbericht respektive Geschäftsbericht. So wird Sicherheit als Beitrag zum Geschäftserfolg und nicht nur als Kostenfaktor wahrgenommen.
- Security Awareness darf und wird etwas kosten. Zum Nulltarif gibt es keine Security Awareness. Planen Sie ein jährliches Budget ein.

Unternehmenssicherheit steigern

Investitionen in die Security Awareness der Mitarbeiter tragen wesentlich zur Unternehmenssicherheit und zum Erhalt des Betriebs bei. Diese Massnahmen lassen sich aktiv vermarkten, beispielsweise in Kundenzeitschriften, Newslettern, Geschäftsberichten oder auf der Website. Dieses Engagement in die Informationssicherheit kann ein Unternehmen als positives Reputationsmerkmal betonen. <

Thomas Manser ist Senior Berater und Projektleiter bei der CSP AG.

René Stock ist Senior Berater und Projektleiter bei der CSP AG.