Security Awareness Programm

Technische Schutzmassnahmen alleine reichen heute nicht aus, um sich gegen die Bedrohungen aus dem Cyber Space zu schützen. Das richtige Verhalten des Mitarbeitenden muss zu einem Element Ihres Schutzkonzeptes werden. Viele Awareness-Programme zeigen jedoch wenig Wirkung. Unser Ansatz, welcher moderne Erkenntnisse aus der Psychologie, der Motivationstheorie und dem Marketing miteinbezieht, führt dazu, dass Ihr Awareness-Programm greift und Ihre Mitarbeitetenden zum stärksten Glied der Verteidigungskette werden.

Die Kunst eines erfolgreichen Awareness Programmes ist es, Mitarbeitende, welche sich nicht für Security interessieren, dazu zu bringen, sich gegenüber dem Thema zu öffnen und zuzuhören.

Die Herausforderungen

Um sich gegen die steigenden Bedrohungen aus dem Cyber Space zu schützen, fokussieren Unternehmen oft darauf, technische Schutzmassnahmen einzusetzen. Die Erkenntnisse der letzten Jahre haben jedoch gezeigt, dass Technologie alleine nicht ausreicht, um die Angriffe abzuwehren. Denn einerseits sind diese immer schwieriger zu entdecken und andererseits zielen immer mehr Angriffsszenarien auf den Menschen ab. Die Aussicht, ein Preisausschreiben gewonnen zu haben, oder die Angst, dass die Kreditkarte gesperrt werden könnte, bringen Menschen oft dazu, genau das zu tun, was der Angreifer von ihnen will. Um sich gegen dieses Fehlverhalten ihrer Mitarbeitenden zu schützen, müssen Unternehmen zusätzliche teure Schutzmassnahmen implementieren und betreiben – Damit aber wird die Ursache des Problems nicht adressiert.

Die Schaffung eines organisationsweit geförderten Sicherheitsbewusstseins macht die **Mitarbeitenden eines Unternehmens zu einer zusätzlichen, sehr effektiven Schutzschicht gegen Cyber-Bedrohungen**.

Der Schlüssel zum Erfolg

Ein Security Awareness Programm kann nur zum Erfolg führen, wenn die Mitarbeitenden so erreicht werden können, dass sie ihr Verhalten ändern: Sie müssen lernen, sich zuerst bewusst richtig zu verhalten und im Optimalfall sogar unbewusst das Richtige tun.

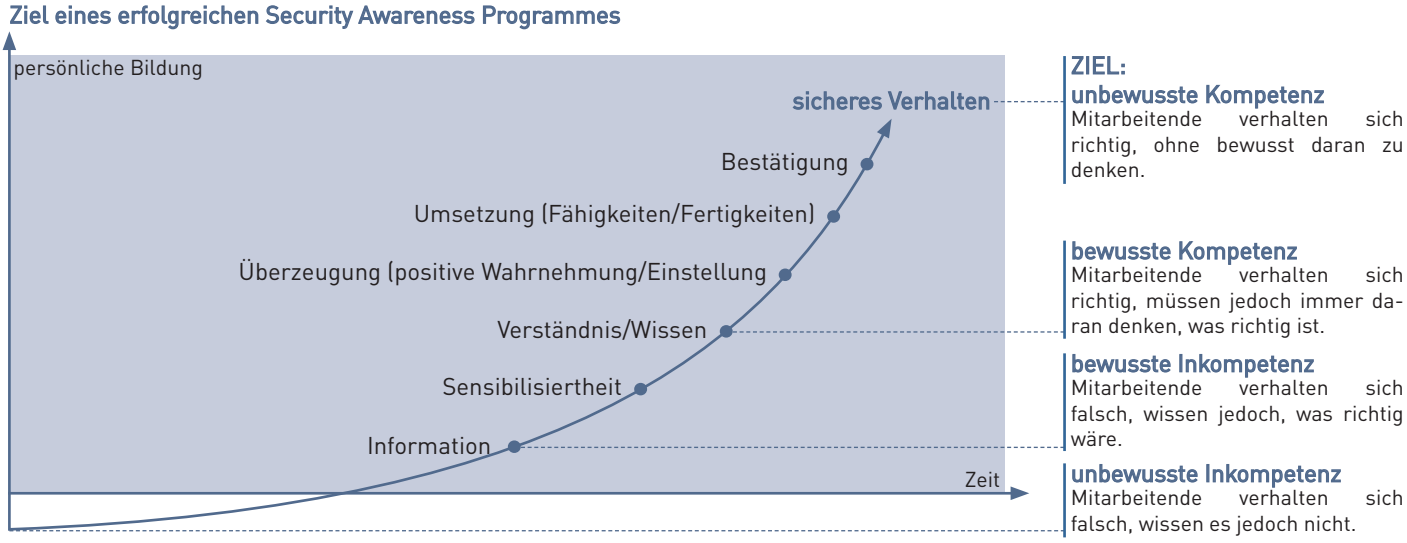
Viele Awareness Programme versuchen, den Mitarbeitenden das richtige Verhalten mit Druck aufzuzwingen. Psychologische Analysen über das Lernverhalten von Menschen haben jedoch gezeigt, dass ein Lernerfolg stark davon abhängig ist, dass sich der Mensch der zu lernenden Thematik öffnet und daran Interesse zeigt.

Das integrale Security Awareness Programm von ISPIN basiert auf einem **interdisziplinären Modell**, welches viele moderne Erkenntnisse aus der Psychologie, der Motivationstheorie, dem Marketing und anderen nicht-technischen Bereichen miteinbezieht.

Der Mensch ist das schwächste und gleichzeitig das stärkste Glied in Ihrer Verteidigungskette.

Zusätzlich wird das Programm an Ihre individuelle Unternehmenskultur angepasst. **Wenn es um Awareness geht, gibt es kein „One Size fits all“.** Massnahmen, welche auf die Kultur Ihrer Unternehmung angepasst sind, haben einen viel höheren Erfolg als Standardmassnahmen.

Ziel eines erfolgreichen Security Awareness Programmes



ISPIN AG ZURICH
swiss made security.

Der ISPIN-Ansatz eines Security Awareness Programmes

Ein Awareness Programm soll folgende Ziele beinhalten:

- **Richtiges Mitarbeiterverhalten bei Risiken und Vorfällen**: Gefahren sollen bekannt gemacht werden, so dass sie von allen Mitarbeitenden rechtzeitig erkannt werden können. Mitarbeitende sollen im Umgang mit Internet, E-Mail etc. sensibilisiert werden.
- **Akzeptanz für Benutzerweisungen und Schutzmassnahmen**: Sicherheitsmassnahmen sollen aktiv von allen Mitarbeitenden unterstützt werden, da sie den Hintergrund und den Nutzen davon vestehen.
- **Stärkung von IT und Informationssicherheit**: Security und die jeweils zuständigen Ansprechpartner sollen beworben werden und so eine positive Wahrnehmung ihrer Aufgaben und Tätigkeiten gefördert werden. Support und Helpdesk sollen entlastet werden.

ISPIN unterstützt, begleitet oder übernimmt die Umsetzung des Security Awareness Programms während dessen gesamter Dauer, kann jedoch auf Wunsch flexibel und etappenweise in einer beratenden oder operativen Rolle mitwirken, um so optimal zum Erfolg beizutragen. Um **eine auf die Kundenorganisation kalibrierte Lösung** mit möglichst hoher Akzeptanz zu entwickeln, gilt das besondere Augenmerk der ISPIN der kundeneigenen Kommunikation mit ihren Kanälen, Plattformen und Massnahmen.

Unsere geschulten Mitarbeitenden unterstützen Sie gerne in der Definition einer Awareness-Strategie und der nachfolgenden Implementation in Ihrer Unternehmung.

Die Phasen eines Awareness Programmes

Phase 1
Analyse & Information

In **Workshops** führen wir Sie durch einen etablierten Prozess, in denen wir den aktuellen **Stand der Security Awareness** innerhalb Ihres Unternehmens erfassen.

Wir machen uns ein Bild Ihrer **Unternehmenskultur**. Vergangene Aktivitäten werden analysiert: Was hat funktioniert, was nicht?

Resultat dieser Phase ist ein **Awarenesskonzept** und eine **Planung** für die nächsten Phasen (Awareness Plan für die nächsten zwei Jahre).

Phase 2
Aufmerksamkeit

In der Aufmerksamkeitsphase werden Mitarbeitende auf allen Stufen auf die verschiedenen Themen der Informationssicherheit aufmerksam gemacht. Mitarbeitende werden durch diverse an Ihre Unternehmenskultur angepasste **Aktivitäten und Massnahmen** an diese verschiedenen Themen herangeführt.

Dabei setzen wir bewusst auf Phasen, in denen aktiv Awareness betrieben wird und auf Ruhephasen. Dies ist wichtig, um **eine Übersättigung** bei den Mitarbeitenden zu **vermeiden**.

Phase 3
Verstärkung & Messung

Themen, welche während der Aufmerksamkeitsphase geschult wurden, werden durch gezielte Wiederholungsmassnahmen **verstärkt und verankert**. Dieses Erinnern an bereits diskutierte Themen verstärkt die Verinnerlichung und festigt das Verhalten der Mitarbeitenden.

Die Veränderung des Verhaltens wird mit gezielten Massnahmen **gemessen**. Je nach Resultat werden Anpassungen an die Schulungsmassnahmen durchgeführt.

Ihr Nutzen

Ausbildung, Sensibilisierung und spürbare Hilfestellungen in den Bereichen der Sicherheit und des Abwehrdispositivs („Corporate Counter-Intelligence") tragen dazu bei, dass Sicherheitsbewusstsein in der Kundenorganisation verankert wird:

- Mitarbeitende auf allen Stufen werden **motiviert**, als Stakeholder die Sicherheit des Unternehmens ernst zu nehmen und kollektiv mitzutragen.
- Die Mitarbeitenden **erkennen** Risiken frühzeitig und verkürzen durch klare Melde- und Ereignisbewältigungsprozesse den Entscheidungsweg und erweitern somit ihre Handlungsfreiheit.
- Sie fühlen sich **befähigt**, mit Herausforderungen korrekt umzugehen und tragen so wesentlich zum integralen Schutz vor technischen und menschlichen Angriffsvektoren bei.
- Strategische Sicherheitsvorgaben, operative Schutzmassnahmen und Weisungen werden besser **verstanden** und aufgrund dessen konsistenter angewendet.
- Die Sicherheitskultur innerhalb Ihres Unternehmens wird kontinuierlich **gestärkt**. Davon profitiert auch die kritische IT- und Informationssicherheit sowie der Gesamtschutz unternehmenseigener Informationen und sensibler Kundendaten.

Kontaktieren Sie uns.

Gerne stellen wir eine massgeschneiderte Offerte für Sie zusammen. Kontaktieren Sie uns für mehr Informationen und Referenzauskünfte.

Craig Fletcher, CCO
+41 44 838 31 11
craig.fletcher@ispin.ch