Sicher digital arbeiten!

Awareness Kampagnen / Mitarbeiter-Sensibilisierung durch Vorträge

IT-Security Awareness der Mitarbeiter

Hacker-Angriffe und IT-Sicherheitsvorfälle sind aktuell in aller Munde und die Medien berichten ausgiebig darüber. In den meisten Unternehmen wird auf aktuelle Bedrohungen reagiert und verschiedene Sicherheitslösungen werden implementiert. Dies wird oft als Einschränkung seitens der Mitarbeiter empfunden. Änderungen sollten im Vorfeld angekündigt werden, ansonsten fehlt es an Akzeptanz durch die Mitarbeiter und Schutzmaßnahmen werden als Behinderung bei der Arbeit wahrgenommen. Oder Schutzmaßnahmen werden unwissentlich umgangen.

Ein guter Weg, Fragen zu IT-Security zu beantworten sind Awareness- bzw. Sensibilisierungs-Veranstaltungen. Hier wird Verständnis für die ergriffenen Sicherheitsmaßnahmen erzeugt, indem die Gründe und die möglichen Risiken erläutert werden. Solche Veranstaltungen sollten im Allgemeinen mindestens die folgenden Anforderungen erfüllen:

Praxis-Relevanz: Risiken und Gefahren sollten realistisch und anschaulich dargestellt und präsentiert werden.

Raum für Fragen: Die Mitarbeiterinnen und Mitarbeiter müssen die Möglichkeit erhalten Fragen zu stellen. Diese Fragen können anonym an die Vortragenden gerichtet werden. Trotz allem sollen auch Diskussionen zwischen den Teilnehmern angestoßen werden.

Klarer Fokus: Es ist ratsam wenige Themen zu behandeln. Dabei werden immer konkrete Lösungen angeboten, die auch praktikabel durchführbar sind.

Unternehmens-Relevanz: Aktuelle, gerade auch auf das Unternehmen bezogene Gefahren sowie aktuelle Sicherheitsvorfälle oder Angriffsversuche sollen nachvollziehbar und anschaulich dargestellt werden.

Die Mitarbeiterinnen und Mitarbeiter müssen sich in den vorgestellten Szenarien wiederfinden und sich der möglichen Gefahren und deren Konsequenzen bewusstwerden.

Zielgruppe

Die Veranstaltungen sollten immer zielgruppengerecht erarbeitet werden. Awareness-Veranstaltungen für das Management haben zum Beispiel einen anderen Fokus als für Mitarbeiterinnen und Mitarbeiter aus den kaufmännischen oder technischen Bereichen.

Mögliche Stufen eines Awareness Projekts

- Kick Off
- Feinplanung der Themen
- Abstimmung der Veranstaltung
- Erste / zweite / n-te Durchführung
- Nachbesprechung

Zeitpunkt

Ein idealer Zeitpunkt für eine Awareness-Veranstaltung kann beispielsweise die Einführung einer neuen Sicherheitsmaßnahme sein. Darüber hinaus sollten aber auch kontinuierlich neue Sensibilisierungs-Themen vorgestellt werden und bereits bearbeitete Schwerpunkte in Erinnerung gerufen und aktualisiert werden.

Durch Wiederholung kann die Nachhaltigkeit der behandelten Themen einer solchen Veranstaltung verstärkt werden.

Mögliche Themen einer Awareness-Schulung

Die Veranstaltung wird an Ihre individuellen Bedürfnisse angepasst und behandelt Ihre aktuellen Themen. Zu jedem Thema werden die von Ihnen präferierten Lösungen vorgestellt.

Wie kommt Malware auf unsere Rechner?

- Welche Varianten des Schadcode-Befalles gibt es und was sind die Anzeichen, die ein Anwender identifizieren kann?

Sichere Passwörter

- Warum sollen Passwörter aus deutlich mehr als vier Zeichen bestehen und eine gewisse Komplexität aufweisen? Warum muss ich es regelmäßig ändern?

Besteht ein höheres Risiko, wenn ich unterwegs bin?

- Wenn ja, warum und wie kann ich dieses Risiko minimieren?

Wie funktioniert Verschlüsselung?

- Welche Notwendigkeit besteht, Dokumente und / oder Daten zu verschlüsseln?
- Wo kann oder muss ich wie verschlüsseln?

Die IT kann aktuelle Sicherheitsbedrohungen nicht alleine bekämpfen. Die IT und die Mitarbeiterinnen und Mitarbeiter sollten an einem Strang ziehen - und zwar in die gleiche Richtung!

Warum Controlware

Informationen sind ein wesentlicher Wert für Unternehmen und Behörden und müssen daher angemessen geschützt werden. Ein vernünftiger Informationsschutz sowie die Grundsicherung von IT und OT sind schon mit verhältnismäßig geringen Mitteln zu erreichen. Informationssicherheit sollte allerdings als laufender Prozess mit Risikoanalyse und Prozessoptimierung verstanden werden um zielgerichtet und möglichst wirtschaftlich in ein Unternehmen oder eine Behörde integriert zu werden.

Die Kombination unserer langjährigen Expertise (Controlware Security seit 1996) mit marktführenden Anbietern von Security-Lösungen steht für erfolgreiche Projekte.

Zusätzlich verschafft uns der höchste Partnerstatus von Controlware bei nahezu allen unseren etablierten Hersteller-Partnern zahlreiche Vorteile, die wir gerne an Sie weitergeben.

Selbstverständlich können Sie auch bei Audits und Zertifizierungen gemäß national und international anerkannter Standards wie ISO 27001, ISO27001 auf Basis IT-Grundschutz / Cobit auf uns bauen.

Mit unseren Controlware Cyber Defense Services erhalten Sie für Ihr Unternehmen modular passende Security Services und mit konkreten Handlungsempfehlungen von unseren erfahrenen Analysten, die zu Ihrer Infrastruktur passen.

Weitere Informationen und Details entnehmen Sie bitte der zugehörigen Leistungsbeschreibung.

Zentrale

Controlware GmbH
Waldstraße 92
63128 Dietzenbach
Tel. +49 6074 858-00
Fax +49 6074 858-108
info@controlware.de
www.controlware.de