LEITFADEN ZUR PLANUNG EINER SECURITY AWARENESS KAMPAGNE

Autor: Martin Braun ISO 27001 Lead Auditor

MB-Factory GmbH - Paul-Mertin-Straße 4b

87629 Füssen Tel. 08362/9241160

www.mb-factory.de

Informationssicherheit nur gemeinsam mit dem Menschen

Im Mittelpunkt der IT-Sicherheitsprozesse steht neben der Technik vor allem der Mensch im Unternehmen – egal in welchem Bereich er tätig ist und welche Position er im Unternehmen bekleidet. Jedoch haben Führungspersonen eine Vorbildfunktion und sollten beim Thema Informationssicherheit mit einem guten Beispiel vorangehen.

Ein ausgefeiltes, erfolgreiches IT-Sicherheitskonzept erfordert vor allem die Einbindung der Mitarbeiter. Neu eingeführte IT-Systeme sowie veränderte Arbeitsprozesse und Verfahren werden besser angenommen, wenn die Anwender den Nutzen der Sicherheitsmaßnahmen und Technologien verstehen. Aus diesem Grund ist die Schaffung bzw. Verbesserung der sogenannten Mitarbeiter Security Awareness unverzichtbarer Bestandteil eines erfolgreichen IT-Sicherheitskonzeptes.

80% aller bekannten Sicherheitsvorfälle werden vom Mitarbeiter unbewusst bzw. bewusst verursacht in dem technische Systeme umgangen werden und Sicherheitsregeln nicht beachtet werden.

Hintergrund hierfür kann der negative Einfluss auf die Mitarbeiterproduktivität sein, welche durch den Einsatz von technischen Schutzsystemen und die Beachtung der neu eingeführten Sicherheitsrichtlinien abnimmt. Somit kann der Mitarbeiter nicht mehr wie gewohnt einfach und schnell seine täglichen Arbeiten durchführen.

Der größte Feind eines jeden Informationssicherheitsprozesses ist der Zwang zur Effektivität, gewohnte Abläufe sowie trainierte Arbeitsabläufe.

Sensibilisierung der Mitarbeiter

Als Security Awareness wird die Sensibilisierung der Mitarbeiter zum vorschriftsmäßigen sowie richtigen Umgang mit Unternehmensdaten jeglicher Art bezeichnet.

Durch Social Engineering-Attacken und Angriffe (Erschleichen von Informationen durch den Mitarbeiter) auf die Informationssicherheit drohen Unternehmen kaum überwindbare Schäden. Eine nachhaltige Sicherheitsstrategie ist unerlässlich – jedoch steckt der Schlüssel zum Erfolg nicht allein in der technischen Absicherung, sondern in sensibilisierten Arbeitskräften. Denn Schäden resultieren meist aus dem Fehlverhalten der eigenen Mitarbeiterinnen und Mitarbeiter.

Während technische Schutzmaßnahmen, wie Virenscanner und Firewalls, zwar viele Angriffe von außen verhindern, schützen diese nicht vor dem Fehlverhalten des eigenen Personals. Sensible Daten werden gestohlen, Kundeninformationen werden herausgegeben oder ausspioniert, unverschlüsselte Laptops und Smartphones gehen verloren. Um Sicherheitsvorfälle dieser Art zu minimieren, gilt es das Bewusstsein der Mitarbeiterinnen und Mitarbeiter nachhaltig zu steigern. Unternehmen benötigen hierzu einen systematischen Ansatz und flexible Awareness-Maßnahmen.

Die wichtigste Voraussetzung um Informationen des Unternehmens zu schützen ist, dass Mitarbeitende Gefahrenquellen erkennen und interne Guidelines verstehen sowie aktiv umsetzen. Mit intelligenten Schulungen, eLearning Systemen sowie durchdachte Kampagnen, können die Richtlinien zur Informationssicherheit nicht nur spannend vermittelt, sondern auch interaktiv trainiert und abgefragt werden. Sinnvoll ist den Mitarbeiter anhand von Situationen und den damit verbundenen Gefahrenquellen zu trainieren, denn nur erlebtes bleibt nachhaltiger und längere Zeit in der Erinnerung der Mitarbeiter. Durch ein aktives Sicherheitsbewusstseins der Angestellten können kostspielige Vorfälle bestmöglich minimiert bzw. verhindert werden. Mitarbeiterinnen und Mitarbeiter sind der zentrale Schlüssel der Informationssicherheit im Unternehmen.

Informationssicherheit Kampagnen als effektives Mittel zur Verbesserung der Mitarbeiter Awareness

Kleine und mittlere Unternehmen achten zu wenig auf IT-Sicherheit. Staatliche Initiativen zur Verbesserung der IT-Sicherheit bei kleinen und mittleren Unternehmen zielen vor allem auf eine erhöhte Wahrnehmung des Themas bei den Unternehmensverantwortlichen ab, geben aber zu wenig konkrete Hilfestellung. Aus diesem Grund ist es essentiell wichtig das Unternehmer sich mit dem Thema Sensibilisierung der Mitarbeiter auseinander setzen und geeignete Maßnahmen und Regeln definieren.

RICHTIG SECURITY AWARENESS KAMPAGNEN PLANEN

Die Basis jeder Security Awareness Kampagne ist eine Sicherheitsrichtlinie mit allen Regeln und Vorgaben in Verbindung mit einer Zieldefinition für die Kampagne. Die wichtigste Frage die gestellt werden muss:

WAS WILL ICH MIT DER KAMPAGNE ERREICHEN?

Vornehmlich ist gezielte Aufklärungsarbeit, zum Beispiel durch Informationsmaterialien, Schulungen oder gezielte IT-Sicherheit Kampagnen zu leisten. Individuelle Beratungen können in den Unternehmen vor Ort entweder durcheigene Mitarbeiter, wie zum Beispiel des Sicherheitsbeauftragten, oder alternativ von externen IT-Dienstleistern durchgeführt werden. Solche Kampagnen lohnen sich, wenn das jeweilige Unternehmen eine Idee oder ein Konzept für die Umsetzung des Vorhabens benötigt.

Eine auf das Unternehmen angepasste IT-Sicherheit Kampagne schafft Bewusstsein bei Mitarbeiterinnen und Mitarbeitern und hilft eine starke Informationssicherheitskultur zu schaffen. Zielsetzung sollte hier auch sein für unterschiedliche Unternehmensbereiche differenzierte Kampagnen durchzuführen!

Warum ist Sensibilisierung so wichtig?

BEISPIEL 1

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hat gegen eine Mitarbeiterin eines Unternehmens ein Bußgeld verhängt, weil sie mit einem offenen E-Mail-Verteiler personenbezogene E-Mail-Adressen einem großen Empfängerkreis übermittelt hat.

Eine Mitarbeiterin eines Handelsunternehmens hat an Kunden eine E-Mail verschickt, die ausgedruckt zehn Seiten umfasst, wobei neuneinhalb Seiten die E-Mail-Adressen ausmachen und eine halbe Seite die Information beinhaltete, dass man sich zeitnah um die Anliegen der Kunden kümmern werde.

E-Mail-Adressen, die sich in erheblichem Umfang aus Vornamen und Nachnamen zusammensetzen, sind als personenbezogene Daten im Sinne des Datenschutzrechts anzusehen. Diese personenbezogenen Daten dürfen an Dritte nur dann übermittelt werden, wenn eine Einwilligung vorliegt oder eine gesetzliche Grundlage gegeben ist. Beide Voraussetzungen lagen hier nicht vor. Die Verwendung dieses offenen E-Mail-Verteilers (Eintragung der EMail- Adressen in das “AN-Feld“) stellte damit einen Datenschutzverstoß dar, der mit einem Bußgeld geahndet werden kann. Im Hinblick auf die erhebliche Anzahl der E-Mail-Adressen hat es das BayLDA in diesem Fall nicht mehr bei einer (folgenlosen) Feststellung der datenschutzrechtlichen Unzulässigkeit belassen, sondern ein Bußgeld verhängt.

Das BayLDA hat bereits unabhängig von diesem Fall mehrfach darauf hingewiesen, dass die Verwendung eines offenen E-Mail-Verteilers datenschutzrechtlich unzulässig ist, wenn die Inhaber der E-Mail-Adressen dazu nicht ihre Einwilligung erklärt haben. Es ist auch dem BayLDA bekannt, dass ein derartiger Verstoß sehr schnell und fahrlässig geschehen kann, wenn man die E-Mail-Adressen in das „AN-Feld“ oder das „CC-Feld“ einträgt und nicht in das „BCC-Feld“. Bei Eintragung der E-Mail-Adressen in das „AN-Feld“ oder das „CC-Feld“ sehen sowohl die unmittelbaren Empfänger („AN-Feld“) als auch die Empfänger der Kopien („CCFeld“) dieser Mail, an wen die Mail sonst noch geschickt wurde. Nur bei Eintragung der EMail- Adressen in das „BCC-Feld“ (englisch: Blind Carbon Copy, dt. sinngemäß Blindkopie) wird die Übertragung der E-Mail-Adressen an die Empfänger unterdrückt, so dass keiner erkennen kann, an wen diese Mail sonst noch geschickt wurde. Da in manchen Unternehmen dieser Fragestellung offensichtlich nicht die entsprechende Bedeutung beigemessen wird, d.h. von Seiten der Unternehmensleitung die Mitarbeiter entweder nicht entsprechend angewiesen oder überwacht werden, wird das BayLDA in einem vergleichbaren Fall in Kürze einen Bußgeldbescheid nicht gegen den konkreten Mitarbeiter, der die Mail mit offenem E-Mail-Verteiler versandt hat, erlassen, sondern gegen die Unternehmensleitung.

Warum ist Sensibilisierung so wichtig?

BEISPIEL 2

Wie kam der Trojaner überhaupt in den Bundestag? Eine Möglichkeit ist, dass die Schadsoftware bewusst oder unbewusst "von innen" eingeschleust wurde. Ende Dezember zum Beispiel wurde der Trojaner Regin auf dem USB-Stick einer Kanzleramtsmitarbeiterin entdeckt. Häufiger als auf Datenträgern verstecken sich Trojaner aber in den Anhängen von E-Mails oder in Dokumenten, die von den jeweiligen Nutzern geöffnet werden, weil sie den Absender für vertrauenswürdig halten. Auch mit dem Besuch von bestimmten Websites können sich Trojaner einnisten. Generell gilt: Je fortgeschrittener die Schadsoftware ist, desto schwieriger ist sie mit gängigen Virenscannern zu entdecken und zu entfernen.

SECURITY AWARENESS

DIE RICHTIGE KAMPAGNE

Eine Security Awareness Kampagne muss für dem Mitarbeiter interessant und einfallsreich gestaltet werden um einen nachhaltigen Erfolg erreichen zu können.

Jeder Mitarbeiter unterscheidet sich in seiner Fähigkeit Lerninhalte aufnehmen zu können und langzeitlich in seinem Gehirn speichern zu können. Aus diesem Grund es wichtig unterschiedliche Lernmethoden miteinander zu kombinieren.

Ein Zitat von Konfuzius sagt

Was du mir sagst, das vergesse ich.

Was du mir zeigst, daran erinnere ich mich.

Was du mich tun lässt, das verstehe ich.

Kombinieren Sie folgende Lern-Methoden – HÖREN – LESEN – AUSFÜHREN

Gehen sie auf die unterschiedlichen Anforderungen und Lernmethoden ihrer Mitarbeiter ein. Stellen Sie ihnen unterschiedliche Lernsysteme, Lernarten und unterstützende Kampagnenmaterialen zur Verfügung um den gewünschten Lernerfolg zu erzielen.

Durch den geeigneten Einsatz von Kampagnenmaterialien bleibt das ERLERNTE beim Mitarbeiter besser in seiner Erinnerung und ist im Arbeitsalltag länger präsent.

Den richtigen Ton treffen – Belehrungen reichen nicht Beispiele schaffen Verständnis und verdeutlichen Folgen. Zeitgemäße Kommunikationsmittel wecken Interesse und helfen Informationen im Unterbewusstsein zu verankern.

Filme, Comics, Flyer und Plakate zeigen das Thema einfach und plakativ auf und können eine Verhaltensänderung herbeiführen. Schulungsunterlagen, Aufkleber und Checklisten erinnern an wichtige Botschaften und Aufgaben. Informationsmaterialien im Corporate Design stärken gleichzeitig die Unternehmenskultur.

Nach der Erarbeitung einer Sicherheitsrichtlinie für das Unternehmen, die grundsätzliche Fragen und Regeln zum Umgang mit Daten im Unternehmen behandelt, muss eine Informationskampagne zur Bekanntmachung folgen.

Schulungsmaßnahmen und Trainings (auch online) können auch komplexere Anforderungen erfüllen. Mit Tests und einer Dokumentation der durchgeführten Maßnahmen können die Verantwortlichen nachweisen, alles aus ihrer Sicht mögliche zur Vermeidung von Sicherheitsrisiken getan zu haben. Das ist im Schadensfall ein wichtiger Punkt. Von besonderer Bedeutung ist die laufende Wiederholung der Maßnahmen sowie Anpassung auf aktuelle Sicherheitsvorfälle.

Übersicht Kampagnen- und Learningmaterialien

Mit E-Learning Kursen kann firmeninternes Knowhow spannend aufbereitet und an Mitarbeiterinnen und Mitarbeiter vermittelt werden. Durch eine virtuelle 3D-Welt und trainieren diese in alltagsbezogenen Situationen korrekte Verhaltensweisen zu Guidelines, gesetzlichen Regelungen etc. Durch unser modernes Design und hochwertige, interaktive Trainingsinhalte wird eine effiziente Bewusstseinsbildung und Wissensvermittlung garantiert.

Auf Ihr Unternehmen angepasste Kampagnen schaffen Bewusstsein bei Ihren Mitarbeiterinnen und Mitarbeitern und helfen eine starke Informationssicherheitskultur zu schaffen. Auf Anfrage können alle Kampagnen Angebote speziell auf Ihre Wünsche zugeschnitten werden. Das Material kann gebrandet und auf Ihre Corporate Identity angepasst werden. Die Exemplare sind als Druck oder als digitale Version inkl. Lizenz erhältlich.

Hier finden Sie einen kleinen Auszug der verfügbaren Materialien, welche Sie bei uns zur Unterstützung ihrer Kampagne erhalten.

SECURITY AWARENESS

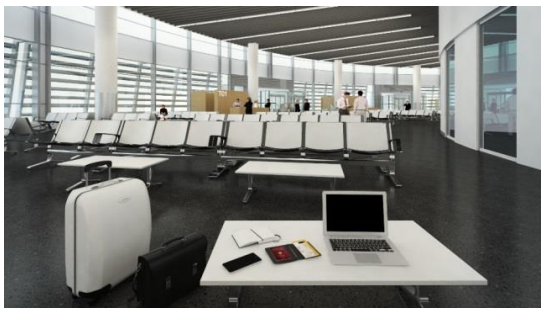
E-LEARNING

Security Awareness Basiswissen

In der Form einer interaktiven Geschichte werden die Mitarbeiter in diesem Training für das Thema Informationssicherheit sensibilisiert.

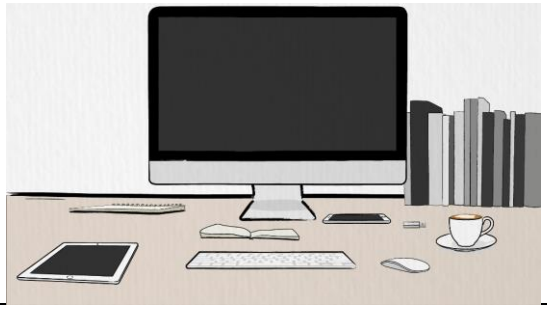
Informationssicherheit auf Reisen

Dieses multimediale Training hilft dabei, Gelerntes im Arbeitsalltag bzw. auf Geschäftsreisen umzusetzen.



Datenschutz

Kurs alle relevanten Definitionen, Begriffe und Grundsätze laut Bundesdatenschutzgesetzes (BSDG).



Informationssicherheit

Mit dem interaktiven Security Awareness Training binden Sie alle Mitarbeiter in den Sicherheitsprozess ein, schulen und sensibilisieren diese.

SECURITY AWARENESS

KAMPAGNENMATERIAL

Security Awareness Quickguide

In diesem kleinen Booklet werden alle wichtigen Sicherheitsvorschriften Ihres Unternehmens kurz und bündig beschrieben und mit Verhaltensrichtlinien untermauert. Als gedruckte oder virtuelle Ausgabe erhältlich

Security Comic Book

Comics sind ein beliebtes Mittel um Schulungsinhalte auflockernd zu vermitteln und um Security Awareness simple zu kommunizieren. Das Comic Buch gibt es als virtuelles Flipbook oder gedruckt

Awareness Poster“COMIC“

Die auf Postern platzierten Comic-Strips vermitteln humorvoll Sicherheitshinweise zur Informationssicherheit in Ihrem Unternehmen.

Awareness Tools

Ob Passworthalter, Screensaver, Viren-Quartett oder andere Quizze – es gibt noch viele weitere Tools, welche Sie bei Ihrer Informationssicherheit-Kampagne unterstützen.

PLANUNG EINER KAMPAGNE

- ## Wer und was?
  - Ist eine interne Sicherheitsrichtlinie vorhanden, die in die Kampagne integriert werden soll?
  - Verantwortlichkeiten klären (Wer ist für welchen Bereich verantwortlich?)
  - Kampagnenname und Slogan, was wollen Sie mit der Kampagne aussagen?

- ## Wie?
  - Auswahl Materialportfolio (Wie wollen wir die Mitarbeiter informieren)
  - Schwerpunkte setzen (Themen wie Verschlüsselung, Klassifizierung)
  - Verteilungsprozess (Wie werden die unterschiedlichen Mitarbeitergruppen informiert).
  - Festlegung der Kursinhalte die vermittelt werden.

- ## Interesse wecken!
  - Information des Management oder des Sicherheitsbeauftragten
  - Verteilung von Broschüren, Veröffentlichung in der Firmenzeitschrift
  - Wechselnde Poster an belebten Stellen (z.B. Kantine; Schwarzes Brett)

- ## Motivieren!
  - Verteilung von Give-Aways
  - Preisausschreiben

- ## Ausbilden und Trainieren!
  - Präsenzschulungen für spezielle Mitarbeiter des Unternehmens.
  - Spezielle eLearning Software die dem Mitarbeiter anhand einer virtuellen Welt die Problemstellungen anhand von Situationen vermittelt und Interaktionen erfordert.

- ## Steuerung und Kontrolle
  - Spezielle eLearning-Kurse mit Tests
  - Quiz

VORBEREITUNG UND DURCHFÜHRUNG EINER KAMPAGNE

Denken Sie in kleinen Schritten! Starten Sie besser zeitnah als jahrelang die optimale Awareness Kampagne vorzubereiten.

Vorbereitung und Identifikation von Themenbereichen

- Initialworkshop
- Sicherstellung der Unterstützung durch die Geschäftsleitung
- Auswahl der Zielgruppe (komplettes Unternehmen, einzelne Abteilungen, Berücksichtigung des jeweiligen Qualifikationsniveaus)
- Bestimmung des Zeit- und Budgetrahmens
- Festlegung des Handlungsbedarfs
- Allgemeine Themen, z.B. Passwortsicherheit, Umgang mit vertraulichen Dokumenten, Virenschutz, Umgang mit Spam E-Mails etc.
- Spezifische Themen, z.B. Verarbeitung personenbezogener Daten, Mobile Sicherheit im Außendienst und bei Heimarbeitsplätzen etc.
- Bestimmung messbarer Erfolgsfaktoren

Festlegung der Kommunikationskanäle und Integration betrieblicher Gremien

- Art der Kommunikation (unter Berücksichtigung der Unternehmenskultur) wie Persönliche Ansprache, Interaktive Elemente, Auswahl von Materialen
- Nutzung etablierter Kommunikationskanäle, z.B. Intranet, E-Mail-Newsletter, Mitarbeiterzeitung etc.
- Integration betrieblicher Gremien wie Geschäftsleitung, Führungskräfte, Mitarbeitervertretung, Meinungsführer im Unternehmen, Betrieblichen Datenschutzbeauftragte, Sicherheitsbeauftragte, Kommunikations- und Presseabteilung

Umsetzung und Visualisierung der Maßnahmen

- Online-Schulungen, z.B. Einsatz von eLearning Lösungen und / oder Präsenzschulungen. Mitarbeiterschulung, Führungskräfte-Schulung, Schulungen für Fachabteilungen (z.B. IT, Personal, Buchhaltung etc.), Spezialschulungen
- Live-Hacking als Spezialmaßnahme
- Begleitung der Kampagne durch Newsletter, Fachvorträge, Factsheets, Hauszeitung, Broschüre/Flyer, Wechselnde Poster an frequentierten Bereichen (z.B. im Eingangsbereich, in der Küche etc.)
- Ansprache und Motivation durch Tools wie Quiz, Videos, Comics zur Einprägung, Beispiele aus der Praxis zu Schadensszenarien, Verteilung von Give-Aways

Erfolgsmessung

- Auswertungen, z.B. Intranetzugriffe
- Tests
- Live-Evaluation (Feedbackgespräche)
- Auswertung von (Online-)Schulungen
- Quiz-Analyse o Social Engineering Angriff
- Techn. Test-Angriff (Fake-E-Mail)

Wiederholung

- Wiederholen Sie laufende Maßnahmen und passen Sie diese auf aktuelle Sicherheitsvorfälle an

>> WEIL BEWUSSTSEIN SICHERHEIT SCHAFFT <<

Dies ist unser Motto und Leitfaden um eine optimale Sensibilisierung Ihrer Mitarbeiter zu erreichen und so Ihre IT Security einen entscheidenden Schritt nach vorne zu bringen.

Wir, ein auf IT-Security und IT Security Awareness spezialisierte Anbieter können auf bewährtes Material zurückgreifen und verfügen vor allem auch über Fachkenntnis, damit Sie schneller und kostengünstiger zu Ergebnissen kommen.

Für weitere Informationen zum Thema IT-Sicherheit, Awareness und Datenschutz kontaktieren Sie uns gerne unter:

MB-Factory GmbH

Tel. 08362/9241160

Info@MB-Factory.de

http://mb-factory.de/it-security-awareness-elearning