LSI-Info A#02

IT-SECURITY-AWARENESS

AWARENESS (ENGL.):
BEWUSSTSEIN, ACHTSAMKEIT, GEWAHRSEIN

Version 1.0 vom: 20.03.2019

Management Summary

Technisch werden von Seiten der IT-Verantwortlichen bereits eine Vielzahl von Maßnahmen (z.B. SPAM- und Phishing-Filter, Virenscanner, Firewalls, Patch-Management etc.) durchgeführt, um Angriffe auf die IT-Systeme zu verhindern. Gleichwohl bieten diese technischen Lösungen keinen 100%igen Schutz vor Angriffen. Vielmehr wird mehr und mehr das Endgerät (und damit der Benutzer) zum direkten Ziel von Angriffen. Somit wird der Mitarbeiter zum wesentlichen Erfolgsfaktor in der IT-Sicherheit. Ein Großteil erfolgreicher IT-Sicherheitsverletzungen wird von Mitarbeitern ausgelöst. Dem Faktor Mensch als potentielles Einfallstor für Schadsoftware (Malware) und Angriffe auf die Informationstechnik kommt somit eine besondere Rolle zu. Security-Awareness-Maßnahmen versuchen, an dieser Stelle für mehr IT-Sicherheit zu sorgen, indem sie den Menschen sensibilisieren.

MOTIVATION ZUR IT-SECURITY-AWARENESS

In vielen anderen Tätigkeitsbereichen sind besondere Sicherheitsunterweisungen längst obligatorisch (z.B. Arbeitsschutzregelungen, Hygienevorschriften etc.). Für den Bereich der Informationstechnik versucht hier die Security-Awareness, diesen Ansatz im Kontext des mitdenkenden Mitarbeiters zu erweitern.

RISIKEN

Durch fehlende Awareness kann ein kleiner Mausklick zum kompletten Stillstand der IT und damit der meisten Geschäftsprozesse führen. Der ungewollte Abfluss von Daten oder die ernsthafte Kompromittierung von IT-Systemen ist häufig mit ernsten Folgen verbunden. Neben messbaren Schäden wie:

- Bekanntgabe von schützenswerten, personenbezogenen Daten (die auch dem Dienst-, Sozial- oder Steuergeheimnis unterliegen können),
- Verlust und/oder Manipulation von Daten,
- Arbeitsunfähigkeit wichtiger Geschäftsbereiche,
- ggf. Schadensersatzforderungen Geschädigter und
- Erpressbarkeit

sind mit jedem IT-Sicherheitsvorfall auch **immaterielle Folgeerscheinungen** verbunden. Hier sind insbesondere zu nennen:

- Imageverlust,
- negative Reputation in den Medien,
- Vertrauensverlust bei den Bürgern und Unternehmen,
- Zweifel an der sicheren Verwahrung von personenbezogenen Daten bei Behörden allgemein und
- Verdacht des unrechtmäßigen Handelns („Datenverkauf“).

ZIELE VON SECURITY-AWARENESS

Jeder Mitarbeiter kann durch Unachtsamkeit und Unwissenheit zum entscheidenden Faktor für einen IT-Sicherheits-Zwischenfall sein. Unabhängig davon, ob Beschäftigte ständig oder nur zeitweise mit IT-Geräten und/oder vertrauenswürdigen Daten arbeiten, sind sie immer dem Risiko ausgesetzt, Ziel eines Angriffs zu werden.

EINE SECURITY-AWARENESS-KAMPAGNE MUSS AUF ALLE MITARBEITER ABZIELEN.

Ziel von Security-Awareness ist es, den Mitarbeiter in das Zentrum der IT-Sicherheit zu rücken und damit das Augenmerk des Mitarbeiters auf potentielle Bedrohungen zu lenken und seine Sinne für Angriffsversuche zu schärfen. Es handelt sich hierbei nicht um eine einmalige Aktion, sondern vielmehr um einen stetigen Prozess der Sensibilisierung (ggf. auch auf veränderte Rahmenbedingungen).

Inhaltlich sind unter Einbeziehung der IT-Landschaft auch arbeitsrechtliche Rahmenbedingungen zu berücksichtigen.

Bei Security-Awareness-Maßnahmen sollte auf folgende Punkte eingegangen werden:

- Grundlagen der Informations- und Datensicherheit (u.a. auch Rechtsnormen BayDSG, DSGVO, BDSG, § 35 SGB I, § 30 AO, etc.)
- Sensibilisierung hinsichtlich der Zugangskontrolle zu Amtsräumen und Gebäuden bzw. Gebäudeteilen
- Sicheres Surfen im Internet
- Umgang mit E-Mails, deren Anhängen und Links
- Gefährdung durch Phishing-Angriffe
- Umgang mit Passwörtern (Aufbau, Richtlinien, Vertraulichkeit)
- Schadsoftware und deren Verbreitungs- und Bedrohungspotenzial
- Aufbewahrung und Zugriffsschutz von Datenträgern
- Sicherer Umgang mit mobilen Datenträgern (USB-Stick, CDs, DVDs)
- Bedrohung durch Nutzung nicht zugelassener Software („Downloads“)
- Social Engineering
- Verhalten beim Erkennen von Gefahren und sicherheitsrelevanten Ereignissen

Zu berücksichtigen sind dabei folgende Rahmenbedingungen:

- Nutzung von Social Media
- Gefahren und Risiken bei der Nutzung mobiler Geräte
- Nutzung von öffentlichen WLAN-Netzen mit dienstlichen Geräten
- Gefährdungen im HomeOffice

DURCHFÜHRUNG VON SECURITY-AWARENESS-MAßNAHMEN

Security-Awareness-Maßnahmen werden in vier Phasen eingeteilt.

PHASE 1: DEN MITARBEITER INS ZENTRUM DER SICHERHEIT STELLEN

In der ersten Phase gilt es, den Mitarbeiter dafür zu sensibilisieren, dass er im Mittelpunkt der IT-Sicherheit steht und dass Sicherheitsvorfälle sich direkt und indirekt auf ihn auswirken können. Es gilt, durch gezielte Information bis hin zum Erschrecken Betroffenheit zu wecken. Der Mitarbeiter sollte dabei erkennen, dass der Umgang mit schützenswerten Daten besondere Schutzmaßnahmen auch seinerseits erfordert. Ein in dieser Phase gefundener Sympathieträger als Teaser (z.B. Comic, Cartoon, etc.) würde einen Bogen über alle Phasen spannen.

SECURITY-AWARENESS-KAMPAGNEN

Die Maßnahmen der Phase 1 werden in der Regel über Security-Awareness-Kampagnen durchgeführt. Hier müssen besonders die arbeitsrechtlichen Rahmenbedingungen berücksichtigt werden. Es wird daher empfohlen, den Datenschutzbeauftragten und die Personalvertretung zu beteiligen.

Der Personenkreis, der über eine Security-Awareness-Kampagne in Kenntnis gesetzt ist, sollte so klein wie möglich gehalten werden. Im Idealfall sollte neben arbeitsrechtlich nötigen Beteiligungen lediglich die Behördenleitung informiert sein.

Beispiele: Türhänger an unverschlossenen Büros, simulierte Phishingmail-Versuche und Versuche von Social Engineering, bei denen versucht wird, Informationen über das Umfeld des Mitarbeiters abzufragen

PHASE 2: WISSEN UND VERSTÄNDNIS FÖRDERN

Durch gezielte Schulungsmaßnahmen (z.B. eLearning-Module, Schulungen, Einweisungen durch die IT-Abteilung und/oder den Informationssicherheitsbeauftragen) sollen die Erkenntnisse aus Phase 1 mit Wissen angereichert werden. Wichtig ist, das Verständnis für die Notwendigkeit des Schutzes der Daten und Systeme zu vermitteln. Praxisbezogene und plastische Beispiele, Rollenspiele sowie Tipps und Tricks im sicheren Umgang helfen, den Anwendern das richtige Verhalten in Gefährdungssituationen zu verinnerlichen. Der in Phase 1 gefundene Sympathieträger kann bei all diesen Maßnahmen am Rande auftauchen.
Beispiele: Schulungen, Live-Hacking, E-Learning, Plakate und Handouts

PHASE 3: AWARENESS-NIVEAU AUFRECHTERHALTEN

Ziel dieser Phase ist es, das Niveau der IT-Security-Awareness durch regelmäßige Maßnahmen aufrecht zu erhalten. Bereits erzieltes Sicherheitsbewusstsein lässt über einen Zeitraum von mehreren Monaten wieder nach. Darüber hinaus bringen neue oder geänderte IT-Services neue Gefahren mit sich. Bei all diesen Maßnahmen in dieser Phase sollte der Sympathieträger unauffällig dabei sein.
Beispiele: regelmäßige Veröffentlichungen im Intranet und Mitarbeiterzeitung, Fortsetzungs-Quiz oder Rätsel, Awareness-fördernde Werbemittel und Give-Aways (Haftnotizblöcke, Türhänger, Kalender)

PHASE 4: AWARENESS-GRAD EVALUIEREN

Der Grad der erreichten Awareness sollte regelmäßig überprüft werden. Bereits in den Phasen 1 und 2 können für eine Bilanzierung des Trainingserfolges sowohl technische Kennzahlen wie auch das Knowhow der User erfasst und analysiert werden. Im Rahmen des Einsatzes eines E-Learning-Moduls kann frühzeitig eine Erfassung des Fortschritts mittels von konkreten Fallbeispielen erfolgen.
Beispiele: Klick-Statistik auf malicious Mail-Anhänge, Zugriffsversuche auf kritische Webseiten (Blacklist), Anzahl der eingehenden / gefilterten / geöffneten SPAM-Mails, Abschluss- „Test“ im E-Learning-Modul.
In dieser Phase ist die Personalvertretung in die Maßnahmen einzubinden.

KONTAKT

Weitere Informationen finden Sie unter:

https://lsi.bayern.de/kommunen/

Für Unterlagen und Beratung wenden Sie sich bitte per E-Mail an:

Beratung-Kommunen@lsi.bayern.de.

Gerne ist das kommunale Beratungsteam auch telefonisch unter 0911/215 49 - 523 für Sie erreichbar.