Transferstelle
IT-Sicherheit im Mittelstand
Einfach. Sicher. Machen.

Typisierter Aktionsplan

Der Weg zu mehr IT-Sicherheit

Szenario „Phishing“

ELITE

Mittelstand-Digital

IT-Sicherheit in der Wirtschaft

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

Sehr geehrte:r Besucher:in des ELITE-Erlebnisortes,

zunächst möchten wir Ihnen sagen, dass wir uns sehr freuen, dass Sie an unserem ELITE-Erlebnisort einfache, pragmatische Erzählgeschichten im Demonstrator-Format durchgespielt haben, um sich mit typischen IT-Angriffen und Gefahren im IT-Sicherheitsbereich vertraut zu machen. Das zeigt uns, dass von Seiten der kleinen und mittelständischen Unternehmen tatsächlich ein großes Interesse daran besteht, sich im IT-Sicherheitsbereich weiterzubilden und resilienter für die Zukunft aufzustellen.

An dem **Szenario „Phishing“** haben Sie gesehen, was passieren kann, wenn reale Angriffe gegen Ihr Unternehmen gerichtet werden. Auf diese Situation sind Sie nun besser vorbereitet!

Zu dem am Stand erfolgreich absolvierten Szenario erhalten Sie darüberhinausgehend in diesem Aktionsplan **themenspezifische Aktionen** mit konkreten Umsetzungsvorschlägen für Ihr Unternehmen.

Die in diesem Dokument empfohlenen Aktionen sind in drei Fokusbereiche – organisatorische, technische und personelle Aktionen – gegliedert und passend zu den im Demonstrator adressierten Themen. Damit Sie direkt mit der Umsetzung der Aktionen starten können, gibt es zu jeder Aktion entsprechende Umsetzungsvorschläge. Diese wurden von den IT-Sicherheitsexperten der Projekte Transferstelle IT-Sicherheit im Mittelstand (TISiM, https://tisim.de) und ELITE (https://elite-projekt.de/) aus dem Angebotskatalog der Transferstelle speziell für das Demonstrator-Szenario ausgewählt.

Über diesen ELITE-Aktionsplan hinausgehend, bietet der Sec-O-Mat (https://sec-o-mat.de/) der Transferstelle einem KMU die Möglichkeit, nach Angabe weniger Unternehmenseckdaten, unternehmensspezifische Empfehlungen zu erhalten, basierend auf den konkreten, für das KMU relevante Schadensszenarien.

Wir hoffen, Sie mit dem ELITE-Erlebnisort zur IT-Sicherheit und den darin für Sie bereitgestellten Demonstratoren - und auch mit diesem Aktionsplan - ein Stück sicherer und besser gegenüber Angriffen aus dem Cyberraum wappnen zu können. Wir freuen uns in jedem Fall über Ihre Rückmeldungen jedweder Art unter der Mailadresse elite-feedback@fraunhofer.de.

Wir wünschen Ihnen gute Geschäfte in einer IT-sicheren und gut vorbereiteten Atmosphäre und verbleiben mit freundlichen Grüßen,

Ihr ELITE-Team und Ihre Transferstelle IT-Sicherheit im Mittelstand (TISiM)



Inhaltsverzeichnis

PERS-3: Sicherheitsbewusstsein steigern

BAK Game [Educational Game, Wissenschaftliches Informationsangebot]

Anbieter: Technische Akademie für berufliche Bildung Schwäbisch Gmünd e. V., Lorcher Straße 119, 73529 Schwäbisch Gmünd, Deutschland

Beschreibung: BAK Game (kurz für Bedrohungsanalyse in KMU durch Gamification) ist ein vom BMWK gefördertes Projekt und eine Kooperation der Technischen Akademie für berufliche Bildung und der Hochschule Aalen. Gegenstand des Projekts ist die Erforschung neuartiger Aus- und Weiterbildungsangebote im Bereich IT-Sicherheit für KMU auf Basis von Gamification. Im ersten umgesetzten Lernspiel „Phishing-Quiz" werden Spielende mit Bedrohungen in Mails vertraut gemacht und lernen, die Warnzeichen bei einer bösartigen Mail zu erkennen.

Preis: kostenlos

Link: BAK Game

NoPhish Videos [Video]

Anbieter: Karlsruher Institut für Technologie, Kaiserstraße 12, 76131 Karlsruhe, Deutschland

Beschreibung: In zwei Videos klärt das Karlsruher Institut für Technologie zum Thema Phishing und betrügerische Nachrichten auf. Beide Videos sind ca. 5 Minuten lang und beinhalten eine allgemeine Einführung, die wichtigsten Regeln zur Erkennung von betrügerischen Nachrichten und anschauliche Beispiele. Die Entwicklung der Videos erfolgte u.a. innerhalb des vom Bundesministerium für Wirtschaft und Energie geförderten Projekts KMU Aware.

Preis: kostenlos

Link: NoPhish Videos

Online-Spiel Phishing Master [Educational Game]

Anbieter: Karlsruher Institut für Technologie, Kaiserstraße 12, 76131 Karlsruhe, Deutschland

Beschreibung: Auf spielerische Art und Weise lernt der Nutzer, Webadressen richtig zu lesen bzw. gefährliche Links und Anhänge zu erkennen. Somit gehört "Phishing Master" zu den Serious Games, da in dem Lernspiel wichtige Bildungsinhalte mit unterhaltsamen Elementen verknüpft sind.

Preis: kostenlos

Link: Online-Spiel Phishing Master

Phishing-Simulation

Anbieter: greenhats, Buchenweg 22, 35096 Weimar (Lahn), Deutschland

Beschreibung: Durch die Phishing-Simulation von greenhats sollen Mitarbeiter:innen für das Thema Phishing geschult und sensibilisiert werden. Dafür werden Zielpersonen mit täuschend echt aussehenden E-Mails aufgefordert, Zugangsdaten preiszugeben. Sollten Mitarbeiter:innen die E-Mail nicht als Phishing erkennen, wird Ihnen aufgezeigt, worauf sie hätten achten müssen.

Preis: 800 € (Bezug auf aktuelle Ereignisse), 1.000 € (Mitarbeiterportal), 1.400 € (Auf individuelle Bedürfnisse angepasst)

Link: Phishing-Simulation

Security Awareness

Anbieter: HanseSecure, Franz-Joseph-Str. 11, 80801 München, Deutschland

Beschreibung: Mit den Phishing-Mail- und Social-Engineering-Angriffen von HanseSecure wird dem Auftraggeber das aktuelle Risiko des Unternehmens bei derartigen Bedrohungen aufgezeigt. Darüber hinaus erhält das Personal eine praxisnahe Schulungsmaßnahme, wodurch sie für die Themen Phishing und Social Engineering sensibilisiert werden.

Preis: Auf Anfrage

Link: Security Awareness

Security Awareness Standortbestimmung

Anbieter: IT-Seal GmbH, Hilpertstr. 31, 64295 Darmstadt, Deutschland

Beschreibung: IT-Seal bietet ein komplettes Spektrum an miteinander verzahnten Produkten zur Mitarbeiter-Sensibilisierung gegenüber Phishing Attacken und anderen Angriffen. Dem KMU, das die Dienstleistung in Auftrag gegeben hat, wird nach Auswertung des Mitarbeiterverhaltens bei Phishing-Angriffen ein Gutachten ausgestellt, das vom IT-Sicherheitsverantwortlichen genutzt werden kann, um über weiterführende Schritte zu entscheiden.

Preis: Auf Anfrage

Link: Security Awareness Standortbestimmung

PERS-4: Schulung durchführen

Betrügerische Nachrichten im Unternehmen - Was Sie über Angriffsmethoden wissen müssen [Webinar]

Anbieter: Mittelstand-Digital Zentrum Hannover, Osteriede 6, 30827 Garbsen, Deutschland

Beschreibung: In diesem Webinar wird auf verschiedene Arten von Nachrichten eingegangen, um für die verschiedenen Vorgehen und Risiken zu sensibilisieren. Anhand eines praktischen Fallbeispiels wird exemplarisch der Ablauf eines Angriffs dargestellt und diskutiert. Anschließend wird gemeinsam mit den Teilnehmenden bearbeitet, wie man betrügerische Nachrichten selbst erkennen kann, welche zusätzlichen Schutzmaßnahmen sinnvoll sind und was bei einem Vorfall zu beachten ist. Dies sind die nächsten Veranstaltungstermine: 11.10.2022 (Online).

Preis: kostenlos

Link: Betrügerische Nachrichten

Schulung - Mitarbeitersensibilisierung

Anbieter: Clausohm-Software GmbH, Neubrandenburger Straße 46, 17039 Neverin, Deutschland

Beschreibung: Die Mitarbeiterschulung der Clausohm-Software GmbH umfasst Vorträge und praktische Übungen zu verschiedenen IT-Sicherheitsthemen, wodurch Mitarbeiter im Unternehmen für Social Engineering Attacken sensibilisiert werden sollen.

Preis: Auf Anfrage (Leistungseinheit und Tagessatz möglich)

Link: Schulung - Mitarbeitersensibilisierung

SoSafe Awareness-Plattform [Website]

Anbieter: SoSafe, Ehrenfeldgürtel 76, 50823 Köln, Deutschland

Beschreibung: Die SoSafe Awareness-Plattform sensibilisiert und trainiert Mitarbeitende im Umgang mit Cyber-Gefahren und IT-Sicherheitsrisiken. Die Plattform hat folgende Features: Awareness-Training, Phishing-Simulation, E-Learning und optionale Add-ons, z.B. zur Meldung von verdächtigen E-Mails.

Preis: 249 € (Jahr (5 bis 100 Mitarbeiter))

Link: SoSafe Awareness-Plattform

Webinare zu IT-Sicherheit [Webinar]

Anbieter: Cyber-Akademie, Kaskelstraße 41, 10317 Berlin, Deutschland

Beschreibung: Unter der Rubrik Aus- und Fortbildung bietet die Cyber Akademie verschiedene Webinare zu vielfältigen Themen und Teilgebieten der IT-Sicherheit, weiterhin zu Digitalisierungsthemen, Datenschutz und Business Continuity - teilweise mit Zertifizierung - an.

Preis: ab 179 € (Webinar)

Link: Webinare zu IT-Sicherheit

TECH-2: Sichere Einstellungen wählen

E-Mail Security

Anbieter: TÜV Rheinland i-sec GmbH, Am grauen Stein, 51105 Köln, Deutschland

Beschreibung: Die E-Mail Security Lösungen der TÜV Rheinland i-sec GmbH bieten Unternehmen eine skalierbare und flexible Lösung für E-Mail-Kommunikationen, die auf die Unternehmensbedürfnisse zugeschnitten wird. Neben Eigenschaften wie Anti-Spam, Anti-Virus, Content-Filter oder Graymailing werden weitere Technologien eingesetzt, um beispielsweise „Zero-Day-Exploits" sowie „Advanced Persistent Threats (APTs)" zu detektieren. Zum Schutz der Authentizität, Integrität sowie Vertraulichkeit werden Verschlüsselungstechnologien basierend auf S/MIME sowie PGP eingesetzt.

Preis: auf Anfrage

Link: E-Mail Security

SecuMail

Anbieter: WortNet, Bürgermeister-Graf-Ring 28, 82538 Geretsried, Deutschland

Beschreibung: SecuMail ist ein Cloud-Service, der E-Mails auf Spam und Malware untersucht und filtert. Der Service kann durch einen Eintrag in der Domainverwaltung vor die existierende Infrastruktur geschaltet werden.

Preis: Dynamische Abrechnung gemäß tatsächlicher Nutzung, min. 49 € / Monat für 49 Mailadressen

Link: SecuMail

NoSpamProxy Protection

Anbieter: Net at Work, Am Hoppenhof 32 A, 33104 Paderborn, Deutschland

Beschreibung: Ähnlich einem Mail-Gateway analysiert die Security-Lösung NoSpamProxy den eingehenden Mail-Traffic in Echtzeit auf Spam und Malware, weist entsprechend eingestufte E-Mails zurück und erstellt darüber Benachrichtigungen an den Absender. Die Software erreicht sehr gute Werte für das „False Positive", wodurch tatsächlich angeforderte und relevante E-Mails sehr selten fälschlicherweise als Spam oder Malware erkannt werden.

Preis: Kosten abhängig von Auftragsgröße

Link: NoSpamProxy Protection

ORG-3: Auf IT-Notfälle vorbereiten

Best-Practice-Beispiel: Überraschungsangriff auf die IT [Broschüre/Flyer (Digital)]

Anbieter: Mittelstand 4.0-Kompetenzzentrum Stuttgart, Nobelstraße 12, 70569 Stuttgart, Deutschland

Beschreibung: In diesem 2-Seiter des Mittelstand 4.0-Kompetenzzentrums Stuttgart wird anhand eines realen Best-Practice-Beispiels beschrieben, wie Unternehmen vorgehen, wenn sie sich mit einem Verschlüsselungsangriff konfrontiert sehen, sowie welche Maßnahmen getroffen werden können, um nicht erneut Opfer eines Cyberangriffes zu werden.

Preis: kostenlos

Link: Überraschungsangriff auf die IT

Cyber-Sicherheitsnetzwerk - Anlaufstelle und Notfallnummer für Betroffene von IT-Sicherheitsvorfällen

Anbieter: Bundesamt für Sicherheit in der Informationstechnik (BSI), Godesberger Allee 185-189, 53175 Bonn, Deutschland

Beschreibung: Das vom BSI seit Ende 2020 aufgebaute Cyber-Sicherheitsnetzwerk (CSN) stellt primär eine Notfall-Telefonnummer und ein entsprechendes Notfall-E-Mail-Postfach also Kontaktstelle für Bürger:innen und Unternehmen nach einem IT-Sicherheitsvorfall bereit. Im Rahmen der Anlaufstelle fungiert das BSI ausschließlich als Vermittler hin zu geeigneten IT-Sicherheits-Dienstleistern, die über ein reaktiv-/situatives Angebots- und Notfall-Management-Portfolio verfügen.

Preis: kostenlos

Link: Anlaufstelle bei IT-Sicherheitsvorfällen

Hinweisschild Verhalten bei IT-Notfällen

Anbieter: Allianz für Cyber-Sicherheit, Godesberger Allee 185-189, 53175 Bonn, Deutschland

Beschreibung: Die IT-Notfallkarte „Verhalten bei IT-Notfällen" ist ein Hinweisschild, analog zum bekannten Format „Verhalten im Brandfall". Die aufgeführten Verhaltenshinweisen bei IT-Notfällen aller Art ermöglichen es Organisationen, vom ersten Moment an die richtigen Entscheidungen treffen zu können. Die IT-Notfallkarte wird als PDF-Dokument mit einem editierbaren Textfeld zum Download zur Verfügung gestellt. In das Feld wird die individuelle Rufnummer bei IT-Notfällen eingetragen.

Preis: kostenlos

Link: Hinweisschild Verhalten bei IT-Notfällen

IT-Notfallplan - Im Ernstfall richtig reagieren [Broschüre/Flyer (Digital)]

Anbieter: Mittelstand-Digital Zentrum Berlin, Potsdamer Straße 7, 10785 Berlin, Deutschland

Beschreibung: Die zweiseitige Checkliste des Mittelstand 4.0-Kompetenzzentrums Berlin unterstützt KMU in der Beantwortung der Frage, wie gut sie im Ernstfall auf digitale Angriffe auf das Unternehmen vorbereitet sind.

Preis: kostenlos

Link: IT-Notfallplan - Im Ernstfall richtig reagieren

Kurz erklärt - 3 Tipps für mehr IT-Sicherheit [Video]

Anbieter: Mittelstand-Digital Zentrum Berlin, Potsdamer Straße 7, 10785 Berlin, Deutschland

Beschreibung: In diesem dreiminütigen Video von _Gemeinsam digital, das Mittelstand 4.0-Kompetenzzentrum Berlin werden drei Tipps für mehr IT-Sicherheit im Unternehmen gegeben.

Preis: kostenlos

Link: Kurz erklärt – 3 Tipps für mehr IT-Sicherheit

Maßnahmenkatalog Notfallmanagement

Anbieter: Allianz für Cyber-Sicherheit, Godesberger Allee 185-189, 53175 Bonn, Deutschland

Beschreibung: Der Maßnahmenkatalog des BSI zum Thema Notfallmanagement richtet sich in erster Linie an Geschäftsführende und IT-Verantwortliche in kleinen und mittleren Unternehmen – unabhängig vom Umfang der vorhandenen IT-Kompetenz. Der Maßnahmenkatalog fokussiert IT-Notfälle und gliedert die ausgewählten Maßnahmen in die vier Phasen Vorbereitung, Bereitschaft, Bewältigung und Nachbereitung.

Preis: kostenlos

Link: Maßnahmenkatalog Notfallmanagement

Unternehmen: Einen Vorfall bewältigen, melden, sich informieren, vorbeugen [Artikel]

Anbieter: Bundesamt für Sicherheit in der Informationstechnik (BSI), Godesberger Allee 185-189, 53175 Bonn, Deutschland

Beschreibung: Die Webseite und ihre weiterführenden Unterseiten beschreiben die Problematik von IT-Sicherheitsvorfällen in Unternehmen. Hinweise beziehen sich dabei auf Endsysteme, Server, Anwendungen und die Verarbeitung von Daten mit diesen IT-Systemen sowie auf den richtigen Umgang mit Sicherheitsvorfällen. Ziel ist es, die Kenntnisse wie auch die Aufmerksamkeit von Unternehmen und Mitarbeitenden in diesem Bereich zu erhöhen. Weiterführende Informationen zur Absicherung von IT-Systemen und zu aktuellen Bedrohungen sind ebenfalls verlinkt.

Preis: kostenlos

Link: Vorbeugung und Behandlung von Sicherheitsvorfällen

Was tun bei einem Sicherheitsvorfall? [Artikel]

Anbieter: Mittelstand-Digital Zentrum Chemnitz, Erfenschlager Straße 73, 09125 Chemnitz, Deutschland

Beschreibung: Der Artikel beschreibt die Thematik von IT-Sicherheitsvorfällen und was im Umgang mit diesen zu beachten ist. Dabei werden Tipps gegeben für eine Vorbereitung und Absicherung gegen IT-Sicherheitsvorfälle, sowie Hinweise, wie ein Vorfall erkannt werden kann und was im Fall eines Vorfalls zu tun ist um die negativen Auswirkungen zu minimieren.

Preis: kostenlos

Link: Was tun bei einem Sicherheitsvorfall?

ORG-5: Über Sicherheitslage informiert bleiben

Awareness-Blog [Blog]

Anbieter: SoSafe, Ehrenfeldgürtel 76, 50823 Köln, Deutschland

Beschreibung: In ihrem Awareness-Blog veröffentlicht SoSafe Artikel rund um das Thema IT-Sicherheit. Die Blog-Beiträge geben u.a. Tipps für mehr Passwortsicherheit, sensibilisieren zu aktuellen Themen wie Homeoffice und erläutert für KMU relevante Angriffe wie Phishing.

Preis: kostenlos

Link: Awareness-Blog

Der IT-Sicherheitsblog für den Mittelstand [Blog]

Anbieter: Deutschland sicher im Netz e.V., Albrechtstraße 10c, 10117 Berlin, Deutschland

Beschreibung: Der Blog von Deutschland sicher im Netz bündelt News zum Thema IT-Sicherheit. Ausgewählte Experten nehmen zu IT-Sicherheitsthemen Stellung und informieren mit ihrem Know-how speziell den Mittelstand.

Preis: kostenlos

Link: Der IT-Sicherheitsblog für den Mittelstand

Sicherheitsbarometer [App]

Anbieter: Deutschland sicher im Netz e.V., Albrechtstraße 10c, 10117 Berlin, Deutschland

Beschreibung: Das Sicherheitsbarometer SiBa ist eine kostenfreie mobile App für Android und iOS. SiBa informiert über Spam-Wellen, Viren, kritische Sicherheitslücken und andere Bedrohungen der digitalen Sicherheit in verbreiteten Programmen und Diensten. Gleichzeitig stellt die App erste Handlungsempfehlungen und Sicherheitstipps bereit.

Preis: kostenlos

Link: Sicherheitsbarometer

PERS-1: Vorbildfunktion als Geschäftsführung leben

Awareness Labor KMU (ALARM) Informationssicherheit [Wissenschaftliches Informationsangebot]

Anbieter: Technische Hochschule Wildau, Hochschulring 1, 15745 Wildau, Deutschland

Beschreibung: Das „Awareness Labor KMU (ALARM) Informationssicherheit" baut innerhalb von drei Jahren ein Gesamtszenario zur Sensibilisierung und Unterstützung von KMU für Informationssicherheit bis hin zu deren Selbsthilfe auf. Im Projekt werden in drei Phasen ein innovatives Prozess-Szenario für Informationssicherheit mit analogen und digitalen erlebnisorientierten Szenarien sowie „Vor-Ort-Angriffen" und weiteren Überprüfungen, wie z. B. Awareness-Messungen, Quiz und Tests entwickelt. Das Gesamtszenario soll zu der dringend notwendigen Sensibilisierung von Führungskräften und Mitarbeitenden in KMU und zu einer gezielten Personalentwicklung führen, wie sie derzeit breitenwirksam noch nicht vorhanden sind. Die primäre Projektbeteiligung ist nach Durchlaufen des Auswahlverfahrens kostenfrei.

Preis: kostenlos

Link: Awareness Labor KMU (ALARM) Informationssicherheit

Best Practices für Phishing-Simulationen

Anbieter: SoSafe, Ehrenfeldgürtel 76, 50823 Köln, Deutschland

Beschreibung: Das White Paper zeigt das Potenzial von Phishing-Simulationen auf und stellt acht Best Practices im Sinne einer auf den Lernerfolg der User ausgerichteten Philosophie vor. Die Best Practices beinhalten die technische Vorbereitung, die Ankündigung, die Anonymität und Lernorientierung, die Individualisierung, die Bereitstellung von Lerninhalten, die Etablierung einer Meldekette, die Kontinuität und Randomisierung und die Rückmeldung an die Empfänger. -Hinweis: Zum Download des White Papers müssen die E-Mail-Adresse, der Nachname sowie die Anzahl der Mitarbeitenden angegeben werden.

Preis: kostenlos

Link: Best Practices für Phishing-Simulationen

Security Awareness Seminar für Endanwender und Führungskräfte [Präsenzschulung]

Anbieter: ManufakturIT GmbH, Gemarkenweg 1, 51467 Bergisch Gladbach, Deutschland

Beschreibung: In diesem wahlweise halb- oder eintägigen Seminar für Endanwender und Führungskräfte informiert der Anbieter ManufakturIT GmbH über gängige Social-Engineering-Angriffe und deren Gefahren und möglichen Auswirkungen. Anhand zahlreicher Beispiele und Szenarien wird aufgezeigt, wie Angreifer die technischen Sicherheitsvorkehrungen in einem Unternehmen umgehen können und was die Konsequenzen davon sein können. Ziel ist eine wirksame Sensibilisierung aller Teilnehmenden dieser Schulung und damit indirekt die Schaffung einer sichereren Unternehmenskultur.

Preis: Auf Anfrage

Link: Security Awareness Seminar