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

Typisierter Aktionsplan

Der Weg zu mehr IT-Sicherheit

Szenario „Ransomware (Infizierte Website)“

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 „Ransomware (Infizierte Website)“** 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

TECH-11: Schadsoftware verhindern

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

IT-Sicherheit für KMU [Webinar]

Anbieter: Swisscom AG, Alte Tiefenaustrasse 6, 3050 Bern, Schweiz

Beschreibung: In diesem Webinar werden unterschiedliche Arten von Cyberbedrohungen erläutert und dargelegt, was Unternehmen dagegen tun können. Es wird aufgezeigt, wo die größten Sicherheitslücken bei kleinen und mittleren Unternehmen bestehen, welche Folgen Cyberangriffe und Datenverlust nach sich ziehen können und wie KMU sich schützen können. Anschließend werden konkrete Maßnahmen aufgezeigt, wie sich ein KMU vor Verschlüsselungstrojanern schützen kann. Hinweis: Die Aufzeichnung des Webinars muss über ein Online-Formular angefragt werden.

Preis: kostenlos

Link: IT-Sicherheit für KMU

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

TECH-1: Software und IT-Systeme aktuell halten

Letec Patch-Management

Anbieter: Letec IT Solutions, Friedbergstrasse 68, 8200 Schaffhausen, Schweiz

Beschreibung: Das Letec Patch-Management aktualisiert alle Software-Module bei allen Clients und zentralen Systemen automatisch und zentral aus der Cloud. Der System-Administrator übernimmt nur noch Kontrollfunktionen und wird dadurch zeitlich stark entlastet.

Preis: Auf Anfrage

Link: Letec Patch-Management

Schwachstellenscan

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

Beschreibung: Der Schwachstellenscan von HanseSecure führt automatisierte Scans auf Systeme durch, um grundlegende Schwachstellen, wie veraltete Software, schlechte Passwörter oder grobe Konfigurationsfehler etc., aufzudecken. Das Vorgehen ermöglicht eine schnelle und effiziente Detektion von zahlreichen „einfachen" Schwachstellen, wodurch das grundlegende Niveau der Informationssicherheit des Unternehmens erhöht werden kann. Im Anschluss erfolgen die Auswertung der Ergebnisse sowie eine Abschlussbesprechung.

Preis: Auf Anfrage

Link: Schwachstellenscan

Softwareupdates - ein Grundpfeiler der IT-Sicherheit [Artikel]

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

Beschreibung: Auf dieser Informationsseite des Bundesamtes für Sicherheit in der Informationstechnik (BSI) werden konkrete Praxistipps für Anwender:innen bereitgestellt, mit dem Schwerpunkt auf Software-Updates von Programmen und Betriebssystem. Die Seite erklärt, warum Updates essenziell sind für eine sichere IT und wie und für welche Software sie – automatisch oder manuell – angewendet werden können. Die Informationen sind geeignet für alle Nutzer:innen, die ihr Endgerät (PC, Tablet, Smartphone) selbst administrieren.

Preis: kostenlos

Link: IT-Sicherheit verbessern durch Softwareupdates

Warum sind Softwareupdates so wichtig? [Artikel]

Anbieter: hagel IT-Services GmbH, Süderstraße 232, 20537 Hamburg, Deutschland

Beschreibung: In dem Artikel wird die Wichtigkeit von regelmäßigen Softwareupdates aufgezeigt, indem das Sicherheitsrisiko durch veraltete Software dargestellt wird. Darüber hinaus werden mögliche Vorkehrungen zur Erhöhung der Sicherheit aufgelistet.

Preis: kostenlos

Link: Warum sind Softwareupdates so wichtig?

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

Cybersecurity Awareness Blog [Blog]

Anbieter: AWARE7, Munscheidstraße 14, 45886 Gelsenkirchen, Deutschland

Beschreibung: Der Blog von AWARE7 bietet über 500 kostenfreie Beiträge zu den Themen Hacking, Malware und Betrugsmaschen im Internet.

Preis: kostenlos

Link: Cybersecurity Awareness Blog

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

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

ID Ransomware [Website]

Anbieter: MalwareHunterTeam, USA

Beschreibung: Dieser Dienst hat das Ziel, Betroffene eines Ransomware-Angriffs dabei zu unterstützen, die Ransomware zu identifizieren und herauszufinden, ob ein bekannter Weg zur Entschlüsselung (und damit zur Wiederherstellung) der Daten existiert. Die Identifikation der Ransomware kann anhand der Lösegeld- und Zahlungsinformation oder einer verschlüsselten Datei erfolgen, die über die Website hochgeladen werden kann, und gibt dem Ratsuchenden Informationen zur gezielten Suche nach möglichen Entschlüsselungsprogrammen.

Preis: kostenlos

Link: ID Ransomware

Ransomware-Hilfe-Seite "No more Ransom" [Website]

Anbieter: Europol, Eisenhowerlaan 73, 2517 KK The Hague, Niederlande

Beschreibung: Die Website liefert schnelle Hilfe für Opfer von IT-Attacken mit Verschlüsselungs-Schadsoftware. Der Hilfesuchende findet zahlreiche Tipps zur Vorbeugung und Anleitungen sowie Links zu IT-Sicherheitsexperten.

Preis: kostenlos

Link: Ransomware-Hilfe-Seite "No more Ransom"

TECH-10: Schwachstellen finden und schließen

CARE-Tool zur Risikoeinschätzung

Anbieter: Kriminologisches Forschungsinstitut Niedersachsen e.V., Lützerodestr. 9, 30161 Hannover, Deutschland

Beschreibung: CARE bietet Unternehmen eine individuelle Risikoeinschätzung in Bezug auf ihre Gefährdung durch Cyberangriffe. Ergänzend erhalten diese im Anschluss auf die Risiken abgestimmte demographische Informationen, kurze Hintergrundinfos sowie Empfehlungen, was sie an IT-Sicherheitsmaßnahmen mit welcher Priorität angehen sollten.

Preis: kostenlos

Link: CARE-Tool zur Risikoeinschätzung

Firmengespräch IT-Sicherheit

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

Beschreibung: Als ersten Schritt in Richtung der Digitalisierung bietet das Mittelstand-Digital Zentrum Hannover für Unternehmen ein kostenfreies Vor-Ort-Gespräch im Betrieb mit einem Experten an. Das Gespräch kann für das Unternehmen relevante Themen der IT-Sicherheit umfassen. So kann der Experte beispielsweise bei der Einschätzung der aktuellen IT-Sicherheit im Unternehmen oder bei konkreten Problemstellungen, zum Beispiel zu sicherer Fernwartung, unterstützen.

Preis: kostenlos

Link: Firmengespräch IT-Sicherheit

Selbstcheck IT-Sicherheit [Webbasierte IT-Sicherheitsanalyse, Website]

Anbieter: Mittelstand 4.0-Kompetenzzentrum Chemnitz, Erfenschlager Straße 73, 09125 Chemnitz, Deutschland

Beschreibung: Die Webseite ermöglichst es dem Nutzenden, anhand von Fragen einen Selbst-Check durchzuführen, um in erster Näherung das Maß der Digitalisierung im eigenen Unternehmen einzuschätzen. Die Fragen betreffen die Kategorien Organisation, Prozesse, Produkte, Arbeit und IT-Sicherheit. Der Nutzende kann das Digitalisierungs-Niveau des eigenen Unternehmens anhand der insgesamt 45 Fragen abschätzen und erhält eine summarische Auswertung, durch die sich in Folge Potentiale für die Entwicklung einer Digitalisierungsstrategie des Unternehmens ableiten lassen.

Preis: kostenlos

Link: Selbstcheck IT-Sicherheit