Kofinanziert von der Europäischen Union

EYESonCS

EyesOnCS
Kompendium – Cyber Security Fälle

Deutsch
Oktober 2023

Projektdaten

Akronym: EyesOnCS

Titel: **Enhancing Cyber Security – Development of trainings using "Escape Room" Model**

Projekt Nr.: 2021-1-DE02-KA220-VET-000033003

Projektdauer: 01. Januar 2022–31. Dezember 2023 (24 Monate)

Programm: Erasmus+, Leitaktion 2: Kooperationspartnerschaften, Berufsbildung

Projekt-koordinator: Fachhochschule des Mittelstands (FHM)

Ausgabe: Oktober 2023

Teilnehmende Projektpartnerorganisationen

Staatlich anerkannte, private Fachhochschule des Mittelstands (FHM)

virtualcampus

AKADEMIE ASW

fb finance & banking Associazione per lo sviluppo organizzativo e delle risorse umane

Bleiben Sie dran!

Folgen Sie uns

Erfahren Sie mehr über das Projekt unter:

www.eyesoncs.eu

Kofinanziert von der Europäischen Union

Von der Europäischen Union finanziert. Die geäußerten Ansichten und Meinungen entsprechen jedoch ausschließlich denen des Autors bzw. der Autoren und spiegeln nicht zwingend die der Europäischen Union oder der Europäischen Exekutivagentur für Bildung und Kultur (EACEA) wider. Weder die Europäische Union noch die EACEA können dafür verantwortlich gemacht werden.

Inhaltsverzeichnis

Abbildungen

1. Einführung in das Thema

Kein Tag ohne Internetkriminalität. Die Cyberkriminalität hat in den letzten Jahren weltweit deutlich zugenommen. Einer der Gründe dafür ist die fortschreitende Digitalisierung in nahezu allen Arbeits- und Lebensbereichen. Während früher Verbrechen und Angriffe durch einen Banküberfall oder einen anderen physischen Angriff gekennzeichnet waren, sind sie heute dadurch gekennzeichnet, dass ein Angreifer mit einem Laptop am Strand sitzt und sich illegal Zugang zum Vertriebssystem einer Bank verschafft, um Lösegeld zu erpressen. Der Branchenverband Bitcom beziffert den Schaden auf mehr als 220 Milliarden Euro pro Jahr. Für kleine und mittlere Unternehmen kann ein Angriff und das Abgreifen von Geschäftsgeheimnissen den wirtschaftlichen Ruin bedeuten (Streim, A., Mann, S. (2021)).

Die Corona-Pandemie hat in kurzer Zeit auch neue Arbeitsformate ermöglicht. Die entsprechenden Schutzmaßnahmen wurden nicht parallel etabliert oder angepasst. Dies eröffnet Wege für Angriffe auf die Sicherheit und Schwachstellen für Angreifer und Täter. Aus diesem Grund ist es von immenser Bedeutung, Mitarbeitende über die Auswirkungen und Folgen eines Cyberangriffs zu informieren und entsprechend zu sensibilisieren.

Dieses Kompendium wurde im Rahmen des Erasmus+ Projekts "EyesOnCS" entwickelt. Das Projektteam verfolgt mit der Entwicklung dieser Publikation mehrere Ziele:
Zunächst werden in einem Überblick Strategien zur Durchsetzung von Cybersicherheit (CS), insbesondere in Klein- und Mittelständischen Unternehmen (KMU), vorgestellt. Anschließend wird auf die besonderen Herausforderungen eingegangen, denen sich KMU bei der Umsetzung von Cybersecurity gegenübersehen. Anschließend geht das Kompendium kurz auf die Bedeutung von Bildung und Ausbildung bei der Abwehr von CS-Angriffen ein. Es folgt eine umfassende Sammlung von Cybersecurity-Fällen, die in der Praxis aufgetreten sind. Diese Fälle wurden von dem internationalen Projektteam bei Unternehmen und anderen Institutionen gesammelt und für dieses Kompendium ausführlich dokumentiert.

Die Zielgruppen für dieses Kompendium sind in erster Linie Unternehmen und Bildungseinrichtungen, die die gesammelten CS-Fälle für Schulungszwecke nutzen können.

Nach einer Einführung in das allgemeine Sicherheitsthema befasst sich das zweite Kapitel mit wichtigen nationalen und europäischen CS-Strategien. In diesem Zusammenhang wird die Rolle der ENISA (European Union Agency for Cybersecurity) erläutert und hervorgehoben. Dazu heißt es im konsolidierten jährlichen Tätigkeitsbericht der ENISA: "Im Jahr 2021 war die ENISA mit den Herausforderungen konfrontiert, die die Pandemie mit sich brachte, was sich auf die Aktivitäten zum Aufbau von Kapazitäten auf mehreren Ebenen auswirkte. Einerseits mussten mehrere Kurse und Übungen aus offensichtlichen Gründen auf Online-Dienste umgestellt werden. Diese Umstellung brachte einige Herausforderungen mit sich".[1]

1 ENISA: Consolidated Annual Activity Report 2021, Attiki, 2022

Darüber hinaus konzentriert sich das Kompendium in diesem Kapitel auf den EU-Cybersicherheitsakt, der einen EU-weiten Rahmen für die Zertifizierung von Produkten, Dienstleistungen und Prozessen der Informations- und Kommunikationstechnologie (IKT) einführt. Unternehmen, die in der EU tätig sind, werden davon profitieren, dass sie ihre IKT-Produkte, -Prozesse und -Dienstleistungen nur einmal zertifizieren müssen und dass ihre Zertifikate in der gesamten Europäischen Union anerkannt werden.[2]

Darüber hinaus versucht das Kompendium in diesem zweiten Kapitel, verschiedene nationale Sicherheitsstrategien zu erfassen und darzustellen. Aus praktischen Gründen ist die Liste nicht erschöpfend und wird laufend ergänzt. Erläutert werden unter anderem die folgenden

- der deutsche Verein "Deutschland sicher im Netz e.V. (DsiN)"[3]
- den CERT-Bund[4], ein Computer Emergency Response Team für Bundesbehörden
- die italienische nationale Cybersicherheitsstrategie für 2022/26 oder
- das portugiesische nationale Zentrum für Cybersicherheit (CNCS).

Das folgende dritte Kapitel fasst die Herausforderungen für KMU im Bereich der Cybersicherheit zusammen. Dazu verwenden die Autoren den dreiteiligen Ansatz der ENISA mit Empfehlungen für KMU[5]. Das aktuelle Kompendium befasst sich mit den folgenden Bereichen:

- Gebiet Menschen
- Bereich Prozesse
- Bereich Technik.

Dieses Projekt zielt darauf ab, bestimmte KMU-Empfehlungen auf Bildungsebene umzusetzen. Die ENISA KMU-Empfehlungen konzentrieren sich auf vier verschiedene Bereiche. Dieses Kompendium enthält Leitfragen für CS-Checkups und auch für die Beurteilung der gesammelten praktischen CS-Fälle (siehe Kapitel 5).

Das vorliegende Projekt zielt darauf ab, spezielle virtuelle CS-Trainingsmethoden zu entwickeln und diese später anhand von sogenannten Szenarien umzusetzen. Daher werden in Kapitel 4 des Kompendiums relevante Konzepte für das CS-Training beschrieben und bewertet. Dazu gehören Game-Based Learning und Educational Escape Rooms (EERs).

Ein besonders wichtiger und umfangreicher Teil des Kompendiums besteht aus der zusammenfassenden Beschreibung und Bewertung von CS-Praxisfällen, die die Projektpartner in ihren jeweiligen Heimatländern Italien, Deutschland und Portugal recherchiert, zusammengestellt und bewertet haben. In Kapitel 5 werden 26 solcher Praxisfälle in einheitlich strukturierter und vergleichender Form beschrieben.

2 UR-Lex: Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), 32019R0881 - EN - EUR-Lex.
3 Deutschland sicher im Netz, https://www.sicher-im-netz.de.
4 Bundesamt für Sicherheit in der Informationstechnik: Computer Emergency Response Team für Bundesbehörden (CERT-Bund),https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html.
5 ibid.

2. Nationale und europäische Strategien

Auf europäischer Ebene befinden sich die Strategien zur Prävention von Cyberkriminalität und zur Cybersicherheit noch in der Entwicklung. Es gibt bereits einige gute Ansätze, aber auch noch viele herausfordernde Aufgaben. Derzeit gibt es nur wenige staatliche Stellen, die sich mit diesem Thema befassen, das für KMU besonders wichtig ist.

Eine dieser Agenturen ist die ENISA (European Union Agency for Cybersecurity)[6]. Sie hat die Aufgabe, zu einem hohen gemeinsamen Niveau der Cybersicherheit in ganz Europa beizutragen. Die ENISA unterstützt aktiv die Politik der Europäischen Union zur Erhöhung der Cybersicherheit und der Vertrauenswürdigkeit von Produkten und Diensten der Informations- und Kommunikationstechnologie durch Cybersicherheitszertifizierung. Darüber hinaus trägt die Agentur dazu bei, die Infrastruktur der Union besser zu verteidigen und letztlich ein sicheres digitales Umfeld für die europäische Gesellschaft und ihre Bürger zu gewährleisten.

Die vergangene Corona-Pandemie hat die Aktivität der europäischen Bürger in verschiedenen Netzen, wie dem Internet, sowohl im beruflichen als auch im privaten Umfeld, weiter erhöht. Leider hat die Pandemie weitere Einfallstore für koordinierte und angepasste Angriffsmethoden geöffnet. Für cyberkriminelle Angreifer ist dies aufgrund des Mangels an ausgeprägten Verteidigungsstrukturen, Know-how und Abwehrmechanismen immer einfacher geworden. Die ENISA hat daraus gelernt und deshalb ihre Aktivitäten zur Verbrechensbekämpfung noch einmal deutlich verstärkt. Dazu heißt es im konsolidierten ENISA-Jahresbericht: "Im Jahr 2021 war die ENISA mit den durch die Pandemie verursachten Herausforderungen konfrontiert, die sich auf die Aktivitäten zum Aufbau von Kapazitäten auf mehreren Ebenen auswirkten. Einerseits mussten mehrere Kurse und Übungen aus offensichtlichen Gründen auf Online-Dienste umgestellt werden. Diese Umstellung brachte einige Herausforderungen mit sich".
Im Jahr 2019 wurde die EU-Agentur für Cybersicherheit durch den EU-Cybersicherheitsakt gestärkt. Er verleiht der Agentur ein dauerhaftes Mandat und stattet sie mit mehr Ressourcen und neuen Aufgaben aus. Nun wird die ENISA eine Schlüsselrolle bei der Einrichtung und Aufrechterhaltung des europäischen Zertifizierungsrahmens für Cybersicherheit spielen, indem sie die technischen Grundlagen für bestimmte Zertifizierungssysteme vorbereitet. Sie beaufsichtigt die Information der Öffentlichkeit über die Zertifizierungssysteme und die ausgestellten Zertifikate über eine spezielle Website. Darüber hinaus hat die ENISA den Auftrag, die operative Zusammenarbeit auf EU-Ebene zu verstärken, den EU-Mitgliedstaaten, die dies wünschen, bei der Bewältigung ihrer Cybersicherheitsvorfälle zu helfen und die Koordinierung der EU im Falle groß angelegter grenzüberschreitender Cyberangriffe und -krisen zu unterstützen.

Darüber hinaus wird mit dem EU-Cybersicherheitsgesetz ein EU-weiter Rahmen für die Zertifizierung von Produkten, Diensten und Prozessen der Informations- und Kommunikations-

6 Bundesamt für Sicherheit in der Informationstechnik: Computer Emergency Response Team für Bundesbehörden (CERT-Bund), https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html.

technologie (IKT) im Bereich der Cybersicherheit eingeführt. Unternehmen, die in der EU geschäftlich tätig sind, werden davon profitieren, dass sie ihre IKT-Produkte, -Prozesse und -Dienstleistungen nur einmal zertifizieren müssen und dass ihre Zertifikate in der gesamten Europäischen Union anerkannt werden. Der EU-Rahmen für die Cybersicherheitszertifizierung von IKT-Produkten ermöglicht die Schaffung von maßgeschneiderten und risikobasierten EU-Zertifizierungssystemen. Er bietet EU-weite Zertifizierungssysteme in Form eines umfassenden Satzes von Regeln, technischen Anforderungen, Normen und Verfahren. Der Rahmen wird auf einer Einigung auf EU-Ebene über die Bewertung der Sicherheitseigenschaften eines bestimmten IKT-Produkts oder -Dienstes beruhen. Es wird bescheinigt, dass IKT-Produkte und -Dienstleistungen, die nach einem solchen System zertifiziert wurden, bestimmte Anforderungen erfüllen.

Auf nationaler Ebene in **Deutschland** unterstützt der Verein "Deutschland sicher im Netz e.V. (DsiN)" Verbraucherinnen und Verbraucher sowie kleine Unternehmen im sicheren und souveränen Umgang mit der digitalen Welt und bietet Lernangebote für Menschen im privaten und beruflichen Umfeld.

Eine weitere sehr lohnende und hilfreiche Unterstützung für KMU ist das CERT-Bund, das Computer Emergency Response Team für Bundesbehörden, das die zentrale Anlaufstelle für präventive und reaktive Maßnahmen bei sicherheitsrelevanten Vorfällen in Computersystemen ist. Neben der Unterstützung für Bundesbehörden bietet das Bürger-CERT kostenlose und neutrale Informationen über aktuelle Angriffe durch Schadsoftware sowie über Sicherheitslücken in Computeranwendungen.

Im Mai 2022 kündigte **Italien** seine nationale Cybersicherheitsstrategie für 2022/26 an, ein wichtiges Dokument, um Cyberbedrohungen zu bekämpfen und die Widerstandsfähigkeit des Landes zu erhöhen. Die von der italienischen Nationalen Agentur für Cybersicherheit entwickelte Strategie umfasst 82 Ziele, mit denen die folgenden Herausforderungen angegangen werden sollen:

- Sicherstellung eines cyberresistenten digitalen Übergangs der öffentlichen Verwaltung (PA) und des Produktivsystems.
- Vorhersage der Entwicklung von Cyber-Bedrohungen, um ihre Auswirkungen auf nationale Infrastrukturen und Organisationen zu verringern.
- Verhinderung von Online-Desinformation in einem breiteren Kontext der hybriden Bedrohung.
- Bewältigung von Cyber-Krisen.
- Stärkung der nationalen und europäischen strategischen Autonomie des digitalen Sektors.

Die italienische Cybersicherheitsstrategie verbindet Sicherheit und Entwicklung im Einklang mit den Werten der italienischen Verfassungscharta. Sie berücksichtigt die Bestimmungen der Cybersicherheitsstrategie der Europäischen Union vom Dezember 2020, den strategischen Kompass der EU für Sicherheit und Verteidigung vom März 2022 und die jüngsten strategischen Leitlinien der NATO. Um diese neue Vision zu verwirklichen, hat Italien ein Cybersicherheitsökosystem konzipiert, das auf der Zusammenarbeit zwischen dem öffentli-

chen und dem privaten Sektor beruht. In einem solchen System wird der aktive Beitrag der Institutionen durch den der Wirtschaftsakteure - vor allem derjenigen, die mit der Verwaltung von Infrastrukturen betraut sind, von denen die Erbringung grundlegender Dienstleistungen durch den Staat abhängt -, der Welt der Universitäten und der Forschung sowie der Zivilgesellschaft ergänzt.[7]

In **Portugal** ist das Nationale Zentrum für Cybersicherheit (CNCS) der operative Koordinator und die auf Cybersicherheit spezialisierte portugiesische Behörde, die mit staatlichen Stellen, Betreibern wesentlicher Dienste und Anbietern digitaler Dienste zusammenarbeitet, um sicherzustellen, dass der Cyberspace als Raum der Freiheit, der Sicherheit und des Rechts zum Schutz aller Bereiche der Gesellschaft genutzt wird.[8] Aufgabe des CNCS ist es, zur freien, zuverlässigen und sicheren Nutzung des Cyberspace in Portugal beizutragen, und zwar durch die kontinuierliche Verbesserung der nationalen Cybersicherheit und der internationalen Zusammenarbeit in Abstimmung mit allen zuständigen Behörden sowie durch die Umsetzung von Maßnahmen und Instrumenten, die für die Antizipation, Erkennung, Reaktion und Wiederherstellung von Situationen erforderlich sind, die den Betrieb kritischer Infrastrukturen und nationale Interessen gefährden könnten. CERT.PT koordiniert die Reaktion auf Vorfälle, an denen staatliche Stellen, Betreiber kritischer Infrastrukturen, Betreiber wesentlicher Dienste, Anbieter digitaler Dienste und allgemein der nationale Cyberspace in Portugal beteiligt sind.

7 ACN Italien: Nationale Cybersicherheitsstrategie 2022 - 2026, https://www.acn.gov.it/ACN_EN_Strategia.pdf, gesehen 29.7.22
8 Informationen zur Cybersicherheit: Nationales Zentrum für Cybersicherheit Portugal (CNCS), https://www.cybersecurityintelligence.com/national-cyber-security-centre-portugal-cncs-2730.html.

3. Die Herausforderungen der KMU

Cyberangriffe können kleine und mittlere Unternehmen vor das Aus stellen. KMU sind oft familiengeführte Unternehmen, deren Produktions- und Betriebsgeheimnisse auf einer langen Tradition beruhen. Dies steht in der Praxis oft in erheblichem Gegensatz zu den vorherrschenden Schutzmaßnahmen, die für KMU meist mit erheblichen Kosten verbunden sind und/oder für die es an entsprechendem Know-how fehlt. Die Zahl der Cyberangriffe auf KMU hat in den letzten drei Jahren exponentiell zugenommen. Sie werden auch zunehmend zum Objekt gezielter Wirtschafts- und Industriespionage. In Konzernen mit eigenen Konzernsicherheitsabteilungen sind die Mitarbeiter grundlegend mit dem Thema vertraut. Sie verfügen über ein gewisses Bewusstsein und werden in regelmäßigen Abständen intern geschult. Für den Fall eines Angriffs werden Verantwortlichkeiten und Abläufe benannt und geprobt. All diese Strukturen sind in KMU oft nicht vorhanden. Die meisten Mitarbeiter wissen in der Regel nicht, wie sie mit sensiblen Daten umgehen sollen. Das gefährdet nicht nur die Geschäftsfähigkeit eines Unternehmens, sondern im schlimmsten Fall auch viele Arbeitsplätze. Schließlich sind auch KMU Teil der Lieferkette. Ein erfolgreicher Cyberangriff auf ein KMU kann daher auch große Auswirkungen auf die Lieferkette haben und sich auf eine Regierungsbehörde oder andere größere Unternehmen auswirken.

Laut einer kürzlich durchgeführten Umfrage[9] gaben über 80 % der europäischen KMU an, dass Probleme mit der Cybersicherheit innerhalb einer Woche nach Auftreten des Problems schwerwiegende negative Auswirkungen auf ihr Unternehmen haben würden. 57 % von ihnen gaben an, dass sie höchstwahrscheinlich in Konkurs gehen oder ihr Geschäft aufgeben würden. Trotzdem scheinen die KMU nicht zu begreifen, dass Cybersicherheit nicht nur für größere Unternehmen ein Thema ist. KMU müssen sich daher der Auswirkungen bewusst sein, die Cybersicherheitsprobleme auf ihr Unternehmen haben können. Viele KMU glauben, dass die Sicherheitskontrollen, die in den von ihnen erworbenen IT-Produkten enthalten sind, ausreichen und dass keine zusätzlichen Sicherheitskontrollen erforderlich sind, es sei denn, sie sind durch Vorschriften oder Gesetze vorgeschrieben. Dieses Kompendium soll dazu beitragen, in dieser Hinsicht mehr Klarheit für KMU zu schaffen.

Die ENISA schlägt einen dreifsachen Ansatz mit Empfehlungen für KMU vor[10]:

- Bereich Menschen
- Bereich Prozesse
- Bereich Technik.

Dieses Projekt zielt darauf ab, die folgenden Empfehlungen für KMU auf Bildungsebene umzusetzen. Dazu gehören die Aktualisierung der Software, die Anwendung strenger Zugangskontrollregeln, die Nutzung von Cloud-Diensten und mehr.

9 ENISA: Cybersecurity for SMES- Challenges and Recommendations, Agentur der Europäischen Union für Cybersicherheit (ENISA), Attiki, 2021
10 ebd.

Die ENISA KMU-Empfehlungen[11] konzentrieren sich auf drei verschiedene Bereiche. Innerhalb der Bereiche sind wichtige Prüfpunkte mit Leitfragen aufgeführt. Diese Auflistung kann auch als Fragebogen für einen Selbsttest verwendet werden.

Leitfragen für den Bereich MENSCHEN

Verantwortung	Ist ein Direktor oder eine gleichwertige Person für die Cybersicherheit verantwortlich?
Mitarbeiter-beteiligung	Haben alle Mitarbeiter schriftlich bestätigt, dass sie die Informations-sicherheitspolitik gelesen, verstanden und akzeptiert haben?
Bewusstsein der Mitarbeiter	Werden alle Benutzer Ihrer Computersysteme regelmäßig in ihren Sicherheitsverantwortlichkeiten geschult, um verschiedene Sicher-heitsbedrohungen zu erkennen und mit ihnen umzugehen? Stellen Sie sicher, dass die Mitarbeiter alle Kontaktstellen und Kommunika-tionskanäle kennen und überprüfen können!
Cybersecurity-Schulung	Erhalten die Mitarbeiter mit besonderen Sicherheitsaufgaben eine an-gemessene und regelmäßige Schulung, um ihre Rolle zu unterstützen?
Cybersicherheits-richtlinien	Verfügen Sie über eine dokumentierte Sicherheitspolitik mit zugehö-rigen Betriebsverfahren, die von der Geschäftsleitung unterzeichnet und voll unterstützt wird?
Verwaltung von Drittparteien	Gestattet die Geschäftsleitung Dritten den Zugang zu vertraulichen und/oder wirtschaftlich sensiblen Informationen, solange die entspre-chenden Vertraulichkeitsformulare ausgefüllt sind?

Leitfragen für den Bereich PROZESSE

Prüfungen	Werden kritische Systeme, wie Firewalls und Router, regelmäßig auf Schwachstellen getestet? Werden Computer überprüft, um sicherzu-stellen, dass keine Kopien von illegaler Software vorhanden sind?
Planung und Reaktion auf Vorfälle	Gibt es einen Plan für den Umgang mit Sicherheitsvorfällen?
Passwörter	Werden alle Standardkennwörter auf allen Systemen von den vom Hersteller installierten Standardkennwörtern zurückgesetzt? Werden die Benutzer gezwungen, komplexe und schwer zu erratende Pass-wörter zu verwenden?

11 ebd.

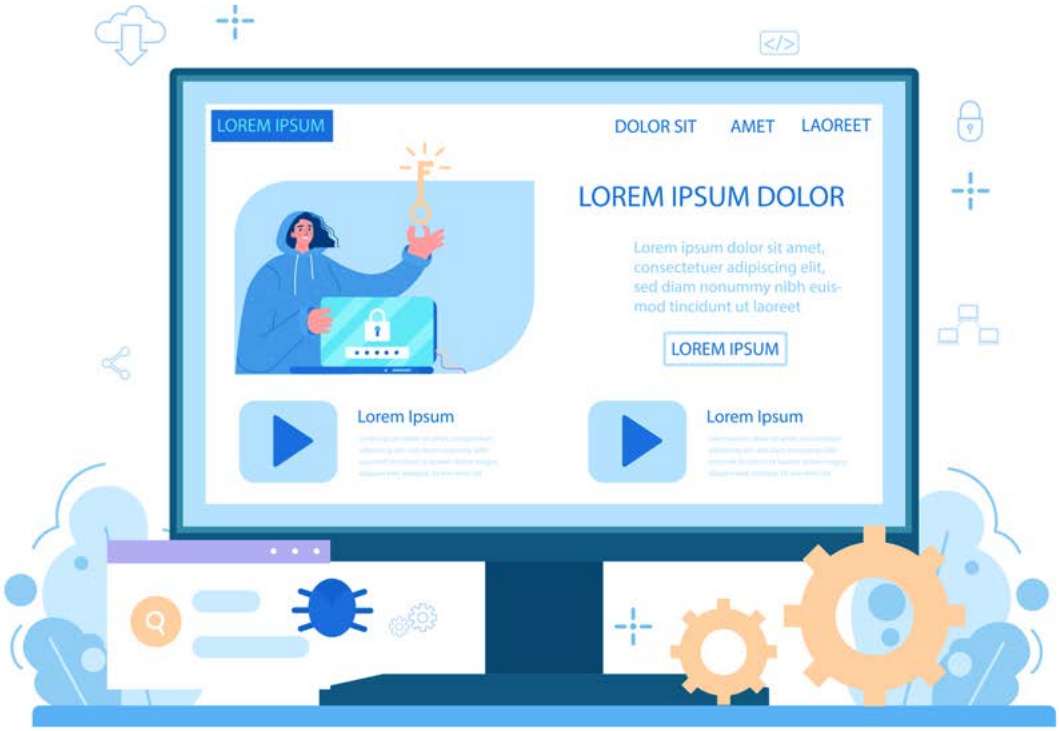
Software-Patches	Gibt es einen Mechanismus, der sicherstellt, dass kritische Sicherheits-Patches rechtzeitig und kontrolliert auf die Systeme aufgespielt werden?
Datenschutz	Sind die Systeme und Datenbanken, in denen personenbezogene Daten gespeichert werden, ordnungsgemäß gesichert, um die Einhaltung gesetzlicher und behördlicher Vorschriften wie der EU-Datenschutzgrundverordnung, des Cybersicherheitsgesetzes[12] und des Datenschutzgesetzes zu gewährleisten?

Leitfragen für den Bereich TECHNIK

Sicherheit im Netz	Sind externe Verbindungen, z. B. zum Internet, von der Geschäftsleitung genehmigt, ordnungsgemäß dokumentiert und durch Firewalls gesichert?
Antiviren-programm	Sind alle Computersysteme mit der aktuellsten Antivirensoftware geschützt? Werden die Nutzer darin geschult, wie sie verdächtige E-Mails oder Dateien, die Computerviren enthalten könnten, erkennen und damit umgehen können?
Verschlüsselung	Wird auf allen Geräten, auf denen Daten gespeichert werden, eine vollständige Festplattenverschlüsselung erzwungen? Verwenden Sie virtuelle private Netzwerke (VPNS), wenn Sie über das Internet in öffentlichen Netzen kommunizieren?
Überwachung der Sicherheit	Werden die Protokolldateien wichtiger Sicherheitsgeräte aktiv überwacht, um mögliche Sicherheitsverletzungen zu erkennen?
Physische Sicherheit	Sind kritische IT-Ressourcen, wie z. B. Dateiserver, in einem gesicherten Bereich untergebracht, der vor unbefugtem Zugriff geschützt ist? Gibt es Maßnahmen im Home-Office, die vergleichbar gesicherte Bereiche wie im Büro gewährleisten (geschlossene Türen beim Verlassen des Arbeitsplatzes, kein Zugriff Dritter auf Informationen über Fenster o. ä.)?
Sichere Backups	Ein gutes Backup kann Ihr Unternehmen vor einem Ransomware-Angriff bewahren. Sichern Sie regelmäßig wichtige Daten und Systeme auf einem sicheren Offline-Speicher? Testen Sie regelmäßig die Wiederherstellung aus Ihren Backups, um sicherzustellen, dass Sie Ihre Daten und Systeme vollständig wiederherstellen können?

12 Europäische Kommission: Der EU-Zertifizierungsrahmen für Cybersicherheit, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework.

4. Rolle von Bildung und Ausbildung – Relevante Konzepte für das Cybersecurity Training



Dass erfolgreiche Cybersicherheit nicht nur vom technischen Schutz abhängt, sondern in hohem Maße auch von der Sensibilisierung und Handlungssicherheit der Mitarbeiter, wird von den Unternehmen nicht immer erkannt. Obwohl jedes vierte Unternehmen kontinuierlich den Handlungsbedarf in der Unternehmenssicherheit identifiziert und mehr Ressourcen zur Verfügung stellt, liegt der Fokus eindeutig auf dem technischen Schutz. In KMU findet die Schulung und Sensibilisierung der Mitarbeiter oft nur in geringem Umfang statt. Damit wird dem Schutzfaktor Mensch, der beim mobilen Arbeiten und im Home Office noch wichtiger wird, zu wenig Beachtung geschenkt. Die Sensibilisierung für die Sicherheitsrisiken, die mit flexiblen Arbeitsplätzen verbunden sind, gewinnt zunehmend an Bedeutung. Natürlich ist es wichtig, die Unternehmen für die neuen Angriffsmöglichkeiten zu sensibilisieren, die sich durch mobile Arbeit und Home-Office ergeben können.

Es ist daher ratsam, Schulungen anzubieten, die sich mit diesem Thema befassen. Darüber hinaus ist es sinnvoll, Unternehmen durch schriftliche Informationen oder Vorträge von Institutionen zu sensibilisieren.

4.1 Spielbasiertes Lernen

Videospiele kamen vor etwa 50 Jahren auf den Verbrauchermarkt, und ihr gesellschaftlicher Einfluss nahm stetig zu, bis sie zu einem grundlegenden sozialen und kulturellen Element wurden (Oblinger 2006). Spiele sind endogene Systeme, deren Problemlösungsaktivitäten

durch Spielmechanismen und Spielregeln strukturiert werden. Das Engagement in Spielen und Spielen ist intern motiviert in dem Sinne, dass Individuen freiwillig an ihnen teilnehmen. Das Engagement der Spieler ist oftmals so stark motiviert, dass sie freiwillig und gern am Spiel teilnehmen. Spiele beinhalten in hohem Maße die Bewertung von Entscheidungen durch den Spieler, was seine Immersion fördert, ein Phänomen, das ein Individuum erlebt, wenn es sich in einem Zustand tiefer geistiger Beteiligung befindet (Agrawal et al., 2020). Spiele tragen aber auch zur Sozialisierung bei und helfen den Spielern, Zusammenhänge zwischen Ursache und Wirkung ihrer Entscheidungen herzustellen, was zu kritischem und logischem Denken beitragen kann. Sie verbessern auch verschiedene kognitive, intra- und interpersonelle Fähigkeiten wie Wahrnehmungsvermögen, Aufmerksamkeit, Gedächtnis, visuelle und auditive Analyse und Synthese, Vergleich, Klassifizierung und Verallgemeinerung.

Ursprünglich als einfache Unterhaltungsobjekte gedacht, wurde die Gestaltung und/oder Nutzung von Videospielen für andere Zwecke als logischer Schritt angesehen, um die Motivation und das Engagement, das die Benutzer beim Spielen erfahren, zu nutzen. So werden Videospiele heute für Bildung und Ausbildung, Bewusstseinsbildung, Werbung, Forschungsstudien, öffentliche Gesundheitskampagnen usw. eingesetzt. Diese Spiele, die als Serious Games bezeichnet werden, werden allgemein definiert als "[Spiele], die nicht in erster Linie der Unterhaltung, dem Vergnügen oder dem Spaß dienen" (Michael und Chen 2006, S. 21) oder als "... ein geistiger Wettbewerb, der mit einem Computer nach bestimmten Regeln gespielt wird und der die Unterhaltung nutzt, um die Ziele von Regierungen oder Unternehmen in den Bereichen Ausbildung, Bildung, Gesundheitsfürsorge, soziales Bewusstsein, öffentliche Politik, Krisenmanagement und strategische Kommunikation zu fördern" (Zyda 2005, S. 26). Serious Games erforschen die inhärente Motivation und das Eintauchen der Spieler durch den Einsatz geeigneter Spielmechaniken und -dynamiken, um spezifische Fähigkeiten und Kompetenzen zu entwickeln, dem Nutzer eine gewünschte Information (oder Botschaft) zu übermitteln oder das erworbene Wissen oder Bewusstsein zu verstärken, während der Nutzer in eine unterhaltsame Umgebung eintaucht.

Das Bildungswesen ist der Bereich mit den meisten (erfolgreichen) Beispielen für die Nutzung von Serious Games und hat daher den Begriff "spielbasiertes Lernen" hervorgebracht, der sich auf die Entwicklung von Spielen konzentriert, die mit spezifischen Lernzielen im Hinterkopf konzipiert sind. Die Nutzer können in einer kontrollierten Umgebung "lernen, indem sie etwas tun" und "durch Fehler lernen", was die Entwicklung von Wissen, Fähigkeiten und Kompetenzen unterstützt und sogar Teamarbeit, soziale Fähigkeiten, Führung und Zusammenarbeit verbessern kann (Juzeleniene et al. 2014).

Game-Based Learning zielt darauf ab, Komponenten zu extrahieren, die Spiele attraktiv machen, und diese mit den gewünschten Informationen und Kenntnissen zu kombinieren, die dem Nutzer vermittelt werden sollen, um so eine interaktive Lernquelle zu schaffen, die wiederum jeden Nutzer motiviert, sein eigenes Wissen zu erweitern und sein Studium in einem herausfordernden, ansprechenden und unmittelbaren Ansatz zu vertiefen (Prensky, 2003). Die folgenden Vorteile wurden mit dem Einsatz von Lernspielen in Verbindung gebracht (Abt, 1987):

- Spiele führen die Nutzer an Probleme und Problemlösungen heran. Spiele können einge-

setzt werden, um die Lernenden zu motivieren, sich an Bildungsprozessen zu beteiligen und sie zu ermutigen, etwas zu schaffen und zusammenzuarbeiten.
- Spiele haben klare Ziele. Wenn sie sorgfältig konzipiert sind, können die Spielziele mit Bildungszielen verknüpft werden und so zum Bildungserfolg beitragen.
- Durch Visualisierung tragen Spiele zu einem besseren Verständnis abstrakter Konzepte bei.
- Die Spieler schlüpfen in realistische Rollen, entwerfen Strategien und treffen Entscheidungen. Dies trägt zur Entwicklung des kritischen und analytischen Denkens sowie der Problemlösungsfähigkeiten bei.
- Spiele bieten Echtzeit-Feedback. Dies erleichtert das Verständnis für die Folgen ihrer Entscheidungen und deckt die Zusammenhänge zwischen Ursache und Wirkung auf. Dieser Prozess trägt zum Aufbau von Wissen bei.
- Spiele können auch für die Bewertung von Konsequenzen durch die Lernenden in einer sicheren Umgebung eingesetzt werden. Sie können auch bei der authentischen Bewertung eingesetzt werden, d.h. bei Prozessen, die simulieren, wie sie in realen Kontexten verwendet werden.
- Spiele sind nützlich und effektiv für (anfängliche) Schulungen, die gefährliche Prozesse und Praktiken abdecken, oder wenn der Einsatz von physischen Räumen für Schulungen teuer ist.

4.2 Educational Escape Rooms (EERs)

Ein "Escape Room" ist ein Spiel, bei dem ein Team von Spielern in einem oder mehreren Räumen Hinweise entdeckt, Rätsel löst und Aufgaben bewältigt, um innerhalb einer begrenzten Zeitspanne ein Ziel zu erreichen. Die Spiele finden an verschiedenen fiktiven Orten statt, z. B. in Gefängniszellen, Kerkern, Labors und sogar in Raumstationen, je nach dem Thema des Spiels. Die Ziele der Spieler und die Herausforderungen, denen sie begegnen, sind ebenfalls auf dieses Thema abgestimmt.

"Die Entwicklung von Escape Rooms geht auf das Jahr 2007 in Japan zurück, wo sie zu kommerziellen Zwecken eingesetzt wurden. Seit ihrer Einführung in den USA im Jahr 2013 erfreuen sie sich schnell wachsender Beliebtheit (Nicholson, 2015)." (Martina, Richard & Göksen, Sultan, 2020)

Das Spiel beginnt in der Regel mit einer kurzen Einführung in die Spielregeln, die in Form von Video, Audio oder durch einen Spielleiter live übertragen wird. Die Spieler betreten dann einen Raum oder ein Gebiet, wo eine Uhr gestartet wird, die die Zeit begrenzt, die sie für das Spiel benötigen, was normalerweise zwischen 45 und 60 Minuten beträgt. Die Spieler erkunden dann den Raum, finden Hinweise und lösen Rätsel, die es ihnen ermöglichen, im Spiel weiterzukommen. Diese Herausforderungen sind im Allgemeinen eher geistiger als körperlicher Natur, aber für die verschiedenen Arten von Rätseln sind unterschiedliche Kenntnisse und Fähigkeiten erforderlich. Wenn die Spielerinnen und Spieler nicht weiterkommen, können sie über einen Mechanismus nach Hinweisen fragen. Die Hinweise können in schriftlicher, Video- oder Audioform oder durch einen Spielleiter gegeben werden. Die Spieler verlieren, wenn sie nicht in der Lage sind, alle Rätsel innerhalb der vorgegebenen Zeit zu lösen. Ein gutes Ende bedeutet in der Regel, dass die Spieler innerhalb der vorgegebenen Zeit "lebend" entkommen, das Ziel des Raums erreichen oder sogar die Bedrohung oder den Antagonisten

der Geschichte aufhalten können, während ein schlechtes Ende in der Regel bedeutet, dass die Spieler nach Ablauf der Zeit von der treibenden Kraft der Geschichte des jeweiligen Spiels oder einem Antagonisten im Raum des Spieles"getötet" werden. Neben dem Unterhaltungsfaktor können Escape Rooms auch dazu genutzt werden, die Zusammenarbeit, die Teamarbeit und die Teambildung zu fördern.

Virtuelle, digitale oder Online-Escape-Rooms sind digitale Gegenstücke zu Escape-Rooms und finden über einen Computer oder ein Netzwerk statt. Das Team kommuniziert und arbeitet über eine synchrone Online-Plattform wie Zoom zusammen, wobei eine Softwareanwendung verwendet wird, die von einem Spieler ausgeführt und für die anderen freigegeben werden kann oder die eine Beteiligung mehrerer Spieler ermöglicht. Wie bei physischen Escape Rooms lösen die Teams Rätsel und lösen Puzzles in einer bestimmten Zeit. Komplexere digitale Escape Rooms können die virtuelle Realität nutzen, um das Gefühl der Immersion der Spieler zu verstärken.

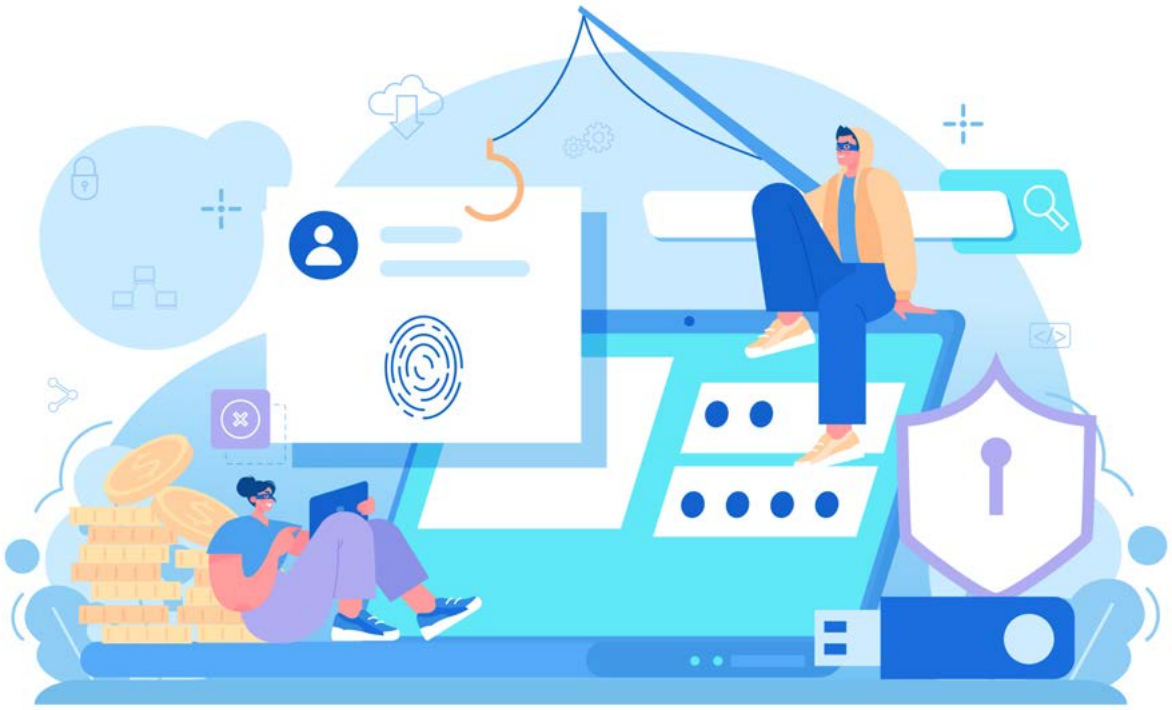
Seit einigen Jahren hat auch der akademische Bereich die Vorteile von Escape Rooms erkannt und nutzt sie für seine Zwecke. Seit einiger Zeit gibt es weltweit verschiedene wissenschaftliche Studien über die Wirksamkeit und den Einsatz von EERs. In Europa gibt es noch nicht allzu viel Forschung zu diesem Thema, aber sie nimmt deutlich zu (Tercanli, H. et al. 2021). Escape-Room-Modelle werden in verschiedenen Themenbereichen eingesetzt. 22% der bisher verwendeten EERs stammen aus dem Bereich der Informatik (Tercanli, H. et al. 2021).

Educational Escape Rooms werden für verschiedene Phasen des Lernprozesses eingesetzt. Während einige EERs keine Vorkenntnisse voraussetzen und das Erlernen der Grundlagen ermöglichen, können andere EERs Vorkenntnisse voraussetzen und das Wissen durch ihren Lehransatz vertiefen (Guckian et al. 2020; Mac Gregor, 2018; Tercanli, H. et al. 2022).

Alles in allem werden durch den Escape-Room-Ansatz Soft-Skills im Allgemeinen gefördert, aber auch die Motivation wird gesteigert und Fähigkeiten wie Problemlösung, Teambildung, Out-of-the-Box-Denken, kritisches Hinterfragen werden eingebracht. Neben den vielen verschiedenen Fähigkeiten wird beim Lernen mit dem Escape-Room-Ansatz auch ein Bewusstsein für ein bestimmtes Thema geschaffen. Es handelt sich also um eine äußerst effektive Lernmethode, die das Wissen der EER-Teilnehmer um ca. 53% signifikant erhöht. Die Festigung des Wissens spielt auch hier eine wichtige Rolle und ist gegeben (Tercanli, H. et al. 2021).

Der Ansatz des Escape-Room-Modells kann auch in Unternehmen sinnvoll eingesetzt werden. Das Projekt EyesOnCS beabsichtigt, die Ausbildung von KMU im Bereich der Cybersicherheit zu unterstützen, indem ein Escape-Room-Ansatz in einer virtuellen Umgebung verwendet wird. Das Projekt und der daraus resultierende Escape Room zum Thema Cybersicherheit sollen das Bewusstsein schärfen und (nicht-technische) Mitarbeiter in ihrem Wissen über das Thema schulen. Dabei wird an den Grundlagen angesetzt und den Spielern durch den Ansatz des spielerischen Lernens ein Gefühl von Sicherheit gegeben. Auch hier soll, wie in der Hochschule, die steile Lernkurve greifen und Motivation für ein Thema gegeben werden, das manchen noch fremd erscheint.

5. Cybersecurity-Fälle



Die Perspektive der Cybersicherheit, insbesondere für KMU und Unternehmen, ist besorgniserregend. Das Schutzniveau der Unternehmen steht in keinem Verhältnis zu den stetig wachsenden digitalisierten Innovationen sowie der Vernetzung digitaler Geräte. Viele Menschen sind auch im privaten Umgang mit Endgeräten zu sorglos und geben unbedacht private und persönliche Informationen im Internet preis. Es ist wichtig, die Gefahren und persönlichen Konsequenzen dieses Verhaltens aufzuzeigen und über den richtigen Umgang mit beruflichen Informationen aufzuklären. Da kleine und mittlere Unternehmen in vielen europäischen Ländern ein Garant für wirtschaftliche Stabilität sind, ist es besonders wichtig, die Mitarbeiter zu sensibilisieren, um Europa ein Stück weit widerstandsfähiger zu machen.

Ein wichtiges Ziel dieses Kompendiums ist es, dem Leser Erfahrungen aus der Cybersicherheitspraxis zu vermitteln. Um dieses Ziel zu erreichen, haben die beteiligten Projektpartner verschiedene Sicherheitsvorfälle zusammengestellt. Diese Sicherheitsvorfälle werden im folgenden Kapitel ausführlich beschrieben.

Die Fälle wurden von allen Partnerorganisationen in allen Partnerländern gesammelt: Italien, Portugal und Deutschland. Die folgenden Kapitel enthalten detaillierte Beschreibungen der Fälle.

5.1 Cybersecurity-Fälle in Italien

Fall 1 – Die Bedeutung von Firewalls für die Cybersicherheit

Titel	Die Bedeutung von Firewalls für die Cybersicherheit
Quelle des Falles	Post e Italiane PST – Nationale Postdienstleistungsgesellschaft (Italien)
Zeitraum des Auftretens	August 2021
Tags	Unternehmen, Identitätsdiebstahl, E-Mail-Attacke, Phishing
Status	bis Ende August 2021 durch Änderung der Anmeldedaten abgeschlossen
Anwendbarkeit Escape Room	Sehr gut anwendbar: Es handelt sich um einen allgemeinen Fall, der leicht zu verstehen ist

Augen auf Phishing:
Bei Phishing-Angriffen werden massenhaft betrügerische E-Mails an ahnungslose Benutzer gesendet, die von einer zuverlässigen Quelle stammend getarnt sind. Die betrügerischen E-Mails sehen oft legitim aus, verlinken den Empfänger jedoch mit einer bösartigen Datei oder einem Skript, das Angreifern Zugriff auf Ihr Gerät gewährt, um es zu kontrollieren oder Informationen zu sammeln, bösartige Skripte/Dateien zu installieren oder Daten wie Benutzerinformationen, Finanzdaten usw. zu extrahieren.
Phishing-Angriffe können auch über soziale Netzwerke und andere Online-Communities erfolgen.[13]

13 https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks/

Was für ein Angriff war das?
Phishing-Angriff

Schwäche/Verwundbarkeit:
Menschliches Versagen - die Unvorsichtigkeit oder Unwissenheit des Opfers führte zu der Cyber-Bedrohung.

Was ist passiert?
- Unbekannten Cyber-Kriminellen gelang es, den E-Mail-Kontakt des Mitarbeiters, der Opfer des Angriffs wurde, ausfindig zu machen. Das Opfer erhielt eine E-Mail, in der es aufgefordert wurde, seine Anmeldedaten für Office 365 Teams (die im Unternehmen verwendete Online-Plattform) zu aktualisieren.


You don't often get email from ordersender-prod@ansmtp.ariba.com. Learn why this is important

Office365

[redacted]@posteitaliane.it Service Desk

Your credential is due to expire TODAY (Friday, April 8, 2022)

Please take note that you are about to lose access to your mailbox if no action is taken.

Keep Using Current Password

This e-mail originates from posteitaliane.it system. Any distribution, use or copying of this e-mail or the information it contains by other than the intended recipient(s) is unauthorized. Thank you.

Abbildung 1: E-Mail.

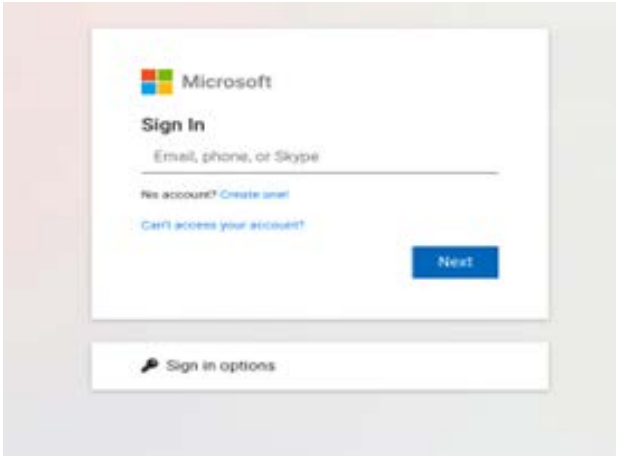


Abbildung 2: Microsoft Log-In.

Das Opfer klickte auf den gefälschten Link in der von den Cyberkriminellen versandten E-Mail und gab die Anmeldedaten für sein Firmenkonto ein.

Wie wurde sie wahrgenommen?

- Das Computer Emergency Response Team (CERT) des Unternehmens entdeckte einige verdächtige Zugriffe aus anderen Ländern wie dem Vereinigten Königreich, Algerien und den Vereinigten Staaten, während sich das Opfer von Mailand in der Lombardei, Italien, aus anmeldete. Dies erregte den Argwohn und das Misstrauen des CERT.

Welche Maßnahmen wurden ergriffen?

- Das CERT forderte das Opfer auf zu bestätigen, dass er sich von diesen Ländern aus in sein Konto eingeloggt hatte. Das Opfer verneinte, woraufhin das CERT ihn aufforderte, seine Anmeldedaten zu ändern.
- Poste Italiane hat ein wirksames Überwachungssystem eingeführt, das auf nationaler Ebene arbeitet. Insgesamt ist die E-Mail-Software des Unternehmens mit einer Firewall ausgestattet, d.h. einem Spam-Filter, der die meisten bösartigen E-Mails abfängt und blockiert.

Was ist das Ergebnis der Verteidigungsmaßnahmen?

Wenn es einer dieser Spam-Mails gelingt, den Filter zu überwinden, haben die Mitarbeiter eine Schaltfläche in ihrer Mailbox, mit der sie die betreffende E-Mail direkt an das CERT melden können. Sobald das CERT die E-Mail analysiert und als bösartig eingestuft hat, extrahiert es die darin enthaltenen Informationen und Links und setzt sie in die Perimeterkontrolle ein, indem es den Zugriff auf den Link blockiert.

Fall 2 – Angriff auf die Lieferkette

Titel	Angriff auf die Lieferkette
Quelle des Falles	ERG Evolving Energies - Italienisches Energieunternehmen
Zeitraum des Auftretens	August 2021
Tags	Unternehmen, Server-Angriff, Datendiebstahl, Malware, Ransomware
Status	innerhalb einer Woche nach Auftreten durch Änderung der Anmeldedaten geschlossen
Anwendbarkeit Escape Room	Nicht zutreffend: Die von der ERG offengelegten Informationen über das Vorgehen der CS-Experten bei der Bewältigung des Hackerangriffs sind nicht detailliert. Daher wäre es schwierig, den Fall zu schildern, insbesondere weil die wichtigsten technischen Aspekte des Angriffs fehlen.

Augen auf Randsomeware:
Ein Ramsomware-Angriff wird hervorgerufen, durch eine Malware, die Verschlüsselung einsetzt, um die Informationen eines Opfers zu erpressen. Die kritischen Daten eines Benutzers oder einer Organisation werden verschlüsselt, so dass sie keinen Zugriff auf Dateien, Datenbanken oder Anwendungen haben. Dann wird ein Lösegeld verlangt, um den Zugriff zu ermöglichen. Im Falle von Ransomware haben Unternehmen nur begrenzte Möglichkeiten:

- das Lösegeld bezahlen
- die gestohlenen Daten zu entschlüsseln
- die gestohlenen Daten zu verlieren/öffentlich zu machen.

Was für ein Angriff war das?
Ransomware

Schwäche/Verwundbarkeit:
Bei Ransomware kann kein "menschliches Versagen" festgestellt werden, da es sich um gezielte Angriffe auf Unternehmen handelt, deren Schutzsysteme von den Tätern im Laufe der Zeit überwacht und studiert wurden.

Was ist passiert?
ERG ist der führende italienische Windkraftbetreiber und gehört zu den zehn größten Onshore-Betreibern auf dem europäischen Markt. Die Gruppe ist in den Bereichen Windenergie, Solarenergie, Wasserkraft und ertragsstarke thermoelektrische Kraft-Wärme-Kopplung tätig. Für ihre IT-Sicherheitsdienste setzt ERG auf Engineering Ingegneria Informatica.

- Nach der Rekonstruktion der Ereignisse durch die Presse schlug die Ransomware-Bande LockBit 2.0 am 30. Julith , 2021 bei Engineering Ingegneria Informatica zu und infizierte deren Server mit einem Virus, der angeblich die Zugangsdaten zu einigen Kunden-VPNs, darunter auch die der ERG, kompromittierte.
- Engineering Ingegneria Informatica meldete den Angriff an seine Kunden und leitete umfangreiche Prüfungen ein, durch die in der Nacht zum 5. Augustth die Matrix und das Ausmaß des Angriffs sowie die gehackten Unternehmen ermittelt wurden. Der Angriff wurde von einer Ransomware namens RansomEXX durchgeführt, die über Engineering Ingegneria Informatica bis zum Computersystem von ERG gelangte.
- Sobald sie in das System eingedrungen waren, kopierten die Cyber-Kriminellen einen Teil der Dateien des Unternehmens und verschlüsselten sie. Die Kriminellen erpressten die ERG öffentlich, indem sie die nachstehende Nachricht auf der Startseite der ERG-Website veröffentlichten und dem Unternehmen damit drohten, die gestohlenen Daten innerhalb weniger Tage preiszugeben, wenn das Unternehmen kein Lösegeld zahle. Der Hauptzweck von Hackerangriffen ist in der Tat der Diebstahl von Daten als Druckmittel für Erpressungsversuche.

Wie wurde sie wahrgenommen?

Während des Angriffs kam es bei der ERG zu einigen begrenzten Unterbrechungen der Informations- und Kommunikationstechnologie (IKT).

Welche Maßnahmen wurden ergriffen?

- Sofortige Aktivierung der internen Cybersicherheitsverfahren: Die ERG hat keine detaillierten Informationen über die technischen Maßnahmen mitgeteilt, die zur Behebung des durch den Angriff verursachten Schadens ergriffen wurden. Sicher ist nur, dass die von der ERG beauftragte CS-Gesellschaft, Engineering Ingegneria Informatica, das Unternehmen aufgefordert hat, die Zugangsdaten zu den Konten zu ändern.
- Anschließend bestätigte die ERG, dass alle Anlagen ordnungsgemäß in Betrieb waren und keine Unterbrechungen auftraten, so dass der Geschäftsbetrieb gewährleistet war.
- Um **den Cyberkriminellen den weiteren Zugriff** auf Unternehmensdaten zu **verwehren**, forderte Engineering Ingegneria Informatica ERG auf, **die Passwörter** der von ihren Teams unterstützten Konten **zu ändern** und jeden anderen Verdacht auf unangemessene Nutzung ihrer Anmeldedaten zu melden.

Was ist das Ergebnis der Schutzmaßnahmen?

Aufgrund des geringen Schadens verweigerte die ERG die Zahlung des Lösegeldes. Nach Angaben der ERG hatten die Hacker Daten verschlüsselt, die als völlig irrelevant angesehen wurden.

Fall 3 – Denial-of-Service-Angriff (DoS)

Titel	Denial-of-Service-Angriff (DoS)
Quelle des Falles	Online-Vermietungsunternehmen (Italien)
Zeitraum des Auftretens	Oktober 2021
Tags	KMU, Unternehmen, Datendiebstahl, Denial-of-Service (DOS)
Status	Der Fall konnte innerhalb einer Woche nach dem Auftreten gelöst werden, indem die Online-Plattform geschlossen und eine neue eingerichtet wurde.
Anwendbarkeit Escape Room	Anwendbar mit Schwierigkeiten: Obwohl es sich um einen häufigen Fall handelt, sind seine Folgen nicht vollkommen reproduzierbar.

Augen auf DoS:
DOS-Angriffe funktionieren, indem sie Systeme, Server und/oder Netze mit Datenverkehr überfluten, um Ressourcen und Bandbreite zu überlasten. Dies führt dazu, dass das System nicht mehr in der Lage ist, legitime Anfragen zu bearbeiten und zu erfüllen. Neben Denial-of-Service-Angriffen (DoS) gibt es auch Distributed-Denial-of-Service-Angriffe (DDoS).
DoS-Angriffe sättigen die Ressourcen eines Systems mit dem Ziel, die Beantwortung von Dienstanforderungen zu verhindern. Andererseits wird ein DDos-Angriff von mehreren infizierten Host-Rechnern aus gestartet, mit dem Ziel, eine Dienstverweigerung zu erreichen und ein System offline zu schalten, um so den Weg für einen anderen Angriff auf das Netzwerk/die Umgebung zu ebnen.[14]

14 https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks/

Was für ein Angriff war das?
Denial of Service (DoS)

Schwäche/Verwundbarkeit
Menschliches Versagen - Der Leiter des Unternehmens war unvorsichtig.

Was ist passiert?
- Bevor das Problem auftrat, hatte sich das vorgestellte Unternehmen gelegentlich auf Sync Security (SS) verlassen, ein privates Cybersicherheitsunternehmen, das auf Datenschutz, Compliance und Geschäftskontinuität spezialisiert ist. Vier Monate vor dem Angriff stellte SS auf der Online-Plattform "Shutdown" fest, dass das betroffene Unternehmen zu den ersten 100 Unternehmen gehörte, die am anfälligsten für Cyberangriffe waren.
- Plattformen wie "Shutdown" melden Daten - die im Laufe der Zeit von Webspidern gesammelt wurden -, die die Art und den Grad der Anfälligkeit der Domänen von Unternehmen angeben und erklären, wie diese Anfälligkeiten ausgenutzt werden können. Diese Plattfor-

men sind für jedermann leicht zugänglich, so dass die Unternehmen, die unter den ersten Hundert rangieren, noch mehr entlarvt werden.
- Es ist in der Tat statistisch erwiesen, dass es innerhalb der ersten 12 Monate nach der Veröffentlichung solcher Reihen zu einem Cyberangriff kommt. Da Angriffe, die auf der Grundlage der von diesen Plattformen veröffentlichten Informationen verübt werden, nicht zielgerichtet sind (bei nicht zielgerichteten Angriffen zielen die Angreifer wahllos auf so viele Geräte, Dienste oder Nutzer wie möglich. Es ist ihnen egal, wer das Opfer ist, da es eine Reihe von Geräten oder Diensten mit Schwachstellen gibt[15]), können sich Unternehmen gegen Cyber-Bedrohungen verteidigen und wirtschaftliche oder Datenverluste verhindern.
- Das SOC (Security Operation System) von Sync Security meldete dieses Risiko daher dem Unternehmensleiter, der das Problem jedoch unterschätzte und sich weigerte, präventive Abwehrmaßnahmen zu ergreifen.
- Vier Monate später wurde die Website des Unternehmens im Bereich der formularbasierten Kundeninteraktion von einem ersten DOS heimgesucht: Unbekannten Cyberkriminellen aus einem - nicht näher bezeichneten - europäischen Land gelang es, die Website zu blockieren und damit ihre Produktivität zu verhindern.

Wie wurde sie wahrgenommen?

In kürzester Zeit wurden die Angriffe gezielter und tiefgreifender, was dazu führte, dass sowohl kommerzielle als auch persönliche Daten der Kunden kompromittiert wurden. Daher forderte der Leiter des Unternehmens das Eingreifen der Experten von Sync Security an.

Welche Maßnahmen wurden ergriffen?

- Das Eingreifen erfolgte sofort: Die Experten von Sync Security leiteten Eindämmungsmaßnahmen ein. Innerhalb von 3-4 Stunden wurde der Angriff noch aggressiver, so dass die ergriffenen Maßnahmen nicht mehr ausreichten, um den Schaden einzudämmen.
- Die Experten von Sync Security trafen mit Erlaubnis des Geschäftsführers des Unternehmens die drastische Entscheidung, den Zugang zur Website für Nutzer außerhalb Italiens zu sperren.
- In der Zwischenzeit wurde das Problem - ein Fehler im Zusammenhang mit dem Code der Website - behoben und Anti-DOS-Schutzmaßnahmen wurden ergriffen. Außerdem nutzten die Experten von Sync Security in den folgenden Tagen eine Plattform zur Überwachung der IP-Bewertung jedes Nutzers.

Was ist das Ergebnis der Schutzmaßnahmen?

- Herunterfahren der Website und Wiedereröffnung, sobald die Bedrohung neutralisiert wurde.
- Die Abschaltung der Website bei Google durch die Hosting-Gesellschaft führte dazu, dass das Unternehmen und seine Mietplattform aus den Browsern verschwanden. Daher musste das Unternehmen Werbekampagnen, Marketingaktivitäten und DEM (Direct Email Marketing) durchführen, die das Verlustbudget weiter belasteten.

15 Nationales Zentrum für Cybersicherheit, https://www.ncsc.gov.uk/information/how-cyber-attacks-work, abgerufen am 20. Januar 2023.

Gelernte Lektionen:
Nach dieser Erfahrung beschloss das Unternehmen, 0,5 % des Umsatzes in Cybersicherheit zu investieren, indem es einen Vertrag mit Sync Security abschloss.

Fall 4 – SQL-Injektion

Titel	SQL-Einschleusung
Quelle des Falles	Versicherungsgesellschaft (Italien)
Zeitraum des Auftretens	Oktober 2021
Tags	KMU, Unternehmen, Diebstahl von Zahlungsinformationen, SQL-Injection
Status	bis Ende November 2021 nach einer technischen Prüfung abgeschlossen.
Anwendbarkeit Escape Room	Nicht zutreffend: Die Informationen darüber, wie die CS-Experten bei der Bewältigung des Hackerangriffs vorgegangen sind, sind nicht detailliert. Daher wäre es schwierig, den Fall zu schildern, zumal es sich um einen Fehlalarm handelte.

Augen auf SQL:
Dies ist der Fall, wenn ein Angreifer mithilfe der Structured Query Language (SQL) einen bösartigen Code in einen Server einfügt und diesen so zwingt, geschützte Informationen zu übermitteln. Bei dieser Art von Angriff wird normalerweise ein bösartiger Schadcode in einen ungeschützten Website-Kommentar oder ein Suchfeld eingegeben. Sichere Kodierungs-Praktiken wie die Verwendung vorbereiteter Anweisungen mit parametrisierten Abfragen sind ein wirksames Mittel, um SQL-Injections zu verhindern.
Wenn ein SQL-Befehl einen Parameter verwendet, anstatt die Werte direkt einzufügen, kann das Backend bösartige Abfragen ausführen. Außerdem verwendet der SQL-Interpreter den Parameter nur als Daten, ohne ihn als Code auszuführen. [16]

16 https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks/

Was für ein Angriff war das?
SQL-Einschleusung

Schwäche/Verletzlichkeit
Menschliches Versagen: Der Nutzer der Website hat einen technisch ungenauen Bericht erstellt.

Was ist passiert?

In den Monaten vor dem Angriff führte die von dem Unternehmen beauftragte Agentur für Cybersicherheit mehrere Penetrationstests durch, um das Sicherheitsniveau des Unternehmenssystems zu bewerten. Obwohl diese Sicherheitstests im Laufe von zehn Tagen im November 2021 gründlich durchgeführt wurden, erhielt das Unternehmen während einer Verkaufsförderungsaktion eine Meldung von einer Verbraucherorganisation, die die Aktion schließlich blockierte.

Wie wurde sie wahrgenommen?

Ein Mitglied der Verbraucherorganisation behauptete, er habe sein Geld verloren, als er seine Zahlungsinformationen auf der Website des Unternehmens eingab.

Welche Maßnahmen wurden ergriffen?

- Der Anwalt des Unternehmens schlug dem Leiter des Unternehmens vor, die Website vom Netz zu nehmen. Es wurde vermutet, dass es sich um einen Fall von SQL-Injection handelte, bei dem ein Cyber-Krimineller mit Hilfe der Server Query Language (SQL) einen bösartigen Code in den Unternehmensserver einfügte und den Server so zwang, geschützte Informationen zu liefern.
- Der Leiter des Unternehmens verlangte eine Erklärung von der Cybersicherheitsagentur: Wie war es möglich, dass das Unternehmen direkt nach einem Penetrationstest Opfer eines Cyberangriffs wurde? Zumal für diese Art von Agenturen Cyberangriffe wie SQL-Injektionen recht einfach zu erkennen sind.
- Die Cybersicherheitsbehörde ergriff sofort Maßnahmen und führte - unter Ausschluss der Öffentlichkeit - auch eine passive Analyse des Berichts durch.
- Der Kunde, der angab, sein Geld bei der Eingabe seiner Zahlungsinformationen auf der Website des Unternehmens verloren zu haben, war ein Student der Computertechnik, der, obwohl er über einige Kenntnisse zu diesem Thema verfügte, durch die Tatsache in die Irre geführt wurde, dass er im HTML-Quellcode der Website des Unternehmens "Injection" las, obwohl es sich dabei nur um eine Funktion der Programmiersprache Java handelt.

Was ist das Ergebnis der Schutzmaßnahmen?

- Die statische Programmanalyse ergab, dass der Angriff nie stattgefunden hat. Der Diebstahl, den der Benutzer erlitt, stand also nicht im Zusammenhang mit der Website des Unternehmens. Es war zwar unwahrscheinlich, dass ein System, das erst vor kurzem einer Druckprüfung unterzogen worden war, eine Schwachstelle aufwies; dies musste jedoch offiziell durch ein technisches Audit überprüft werden.
- Dass die Website vom Netz genommen wurde, bedeutete für das Unternehmen einen großen Einnahmeverlust.

Gelernte Lektionen:
In diesem Fall handelt es sich weniger um einen Fehler, als vielmehr um einen Verdienst. Das Unternehmen - so klein es auch sein mag - erwies sich als vorausschauend, indem es einen professionellen Cybersicherheitsbeauftragten mit der Durchführung von Sicherheitstests beauftragte. Die Investition in die Cybersicherheit hat dem Unternehmen geholfen, das Risiko eines größeren Gewinnverlustes zu vermeiden. Da man sich auf Fachleute verlassen konnte, wurde die Website des Unternehmens unmittelbar nach dem Ergebnis der technischen Analyse innerhalb weniger Stunden wieder in Betrieb genommen. Im Gegenteil, ohne Vorbeugung hätte diese Meldung des Nutzers, die sich schließlich als falsch herausstellte, das Unternehmen das Dreifache an entgangenem Gewinn gekostet, zusätzlich zu den Kosten für den Notfalleinsatz der CS-Spezialisten.

Fall 5 – Smishing

Titel	Smishing
Quelle des Falles	Kleines Einzelhandelsunternehmen
Zeitraum des Auftretens	aufgetreten März 2021
Tags	Unternehmen, Identitätsdiebstahl, SMS-Angriff, Phishing, Smishing
Status	bis Ende März 2021 durch Änderung der Anmeldedaten abgeschlossen.
Anwendbarkeit Escape Room	Sehr gut anwendbar: Es handelt sich um einen alltäglichen Fall, der leicht zu verstehen ist und auf das Escape-Room-Modell übertragen werden kann.

Augen auf Phishing und Smishing:
Smishing ist eine Form des Phishings, bei der Mobiltelefone als Angriffs-Plattform genutzt werden. Der Kriminelle führt den Angriff mit der Absicht durch, persönliche Informationen zu sammeln, einschließlich Sozialversicherungs- und/oder Kreditkartennummern. Smishing wird über Textnachrichten oder SMS durchgeführt, was dem Angriff den Namen "SMiShing" einbrachte. Wenn Cyberkriminelle "Phishing" betreiben, versenden sie betrügerische E-Mails, die den Empfänger dazu verleiten sollen, auf einen bösartigen Link zu klicken. Beim Smishing werden einfach Textnachrichten anstelle von E-Mails verwendet. Im Wesentlichen geht es diesen Cyberkriminellen darum, Ihre persönlichen Daten zu stehlen, die sie dann für Betrügereien oder andere Cyber Straftaten verwenden können.

Was für ein Angriff war das?
Smishing

Schwäche/Verwundbarkeit
Menschlicher Fehler - das Opfer ist in eine Falle getappt. Ihm war nicht klar, dass seine Bank bereits über seine persönlichen Daten verfügte und es daher keinen Grund gab, den Kunden aufzufordern, ein Formular auszufüllen. Und der Kunde wusste offensichtlich nicht, dass eine Bank einen Kunden niemals auffordern würde, Formulare/Logins per E-Mail auszufüllen.

Was ist passiert?
- Den unbekannten Cyber-Kriminellen gelang es, die persönliche Nummer des Mitarbeiters, des Opfers des Angriffs, ausfindig zu machen. Das Opfer hatte eine Hypothekenabtretung beantragt, d. h. es hatte das Verfahren zur Übertragung der Hypothek von einer Bank auf eine andere eingeleitet, wartete jedoch noch darauf, dass ihm seine alte Bank alle erforderlichen Unterlagen zusandte.
- Das Opfer erhielt eine SMS, in der es darüber informiert wurde, dass seine Dokumente auf sein mobiles Bankkonto hochgeladen worden waren, und in der es aufgefordert wurde, auf einen Link zu klicken, um den Download aus dem persönlichen Bereich der Bankwebsite zu starten. Das Opfer nutzte den Unternehmenscomputer, um diesen Vorgang durchzuführen, die Unterlagen herunterzuladen und im Büro auszudrucken. Er klickte auf den Link und wurde auf eine Website umgeleitet, die eine perfekte Kopie der Original-Website war, so dass er sich nicht die Mühe machte, die URL der Website zu überprüfen. Hier wurde er aufgefordert, ein Formular mit seinen persönlichen Daten auszufüllen: Vorname, Nachname, Telefonnummer, Steuernummer.
- Daraufhin erschien die Meldung "Wir haben Ihre Dokumente gesendet", in der das Opfer aufgefordert wurde, auf den Link zu klicken und seine Anmeldedaten einzugeben. Obwohl das Opfer sicher war, die richtigen Anmeldedaten eingegeben zu haben, war das Passwort "falsch". Die Seite, die offenbar gerade aktualisiert wurde, war die echte Seite der Bank.
- Die Kriminellen haben die Anmeldedaten der Bank gestohlen und hatten so Zugang zu den persönlichen Daten des Opfers. Mit den Zugangsdaten gelang es ihnen, das Multifaktor-Authentifizierungssystem zu überwinden, so dass sie das mobile Token-Gerät kontrollieren und Überweisungen direkt vom persönlichen Bereich der Bank-Website aus autorisieren konnten.

Wie wurde sie wahrgenommen?
Als sich das Opfer nach einigen Stunden mit seinem Smartphone in die mobile App der Bank einloggte, stellte es sofort fest, dass sein Kontostand niedriger war.

Welche Maßnahmen wurden ergriffen?
- Das Opfer änderte die Anmeldedaten und informierte das Bankinstitut, dass es Opfer einer Phishing-Kampagne geworden war.

- Er berichtete auch innerhalb des Unternehmens über den Angriff. Das Unternehmen beauftragte einen Cybersicherheitsspezialisten mit einer eingehenden Analyse des Systems, um festzustellen, ob einer der Links, auf den das Opfer geklickt hatte, Malware oder eine andere Bedrohung für die Datenbank des Unternehmens heruntergeladen hatte. Bei der technischen Analyse wurde kein Virus entdeckt: Die Unternehmensdaten waren sicher.

Was ist das Ergebnis der Schutzmaßnahmen?

Die Situation wurde durch Änderung der Anmeldedaten gelöst. Allerdings war das Opfer nicht in der Lage, das Geld zurückzubekommen. Er hätte sich mit der Bank in Verbindung setzen sollen, um sich von der Richtigkeit der SMS zu überzeugen. Außerdem hätte er den Firmencomputer nicht zur Erledigung seiner persönlichen Angelegenheiten nutzen dürfen, auch wenn es dringend war. In diesem Fall ist auch die psychologische Seite der Situation zu berücksichtigen: Hypotheken sind heikle Angelegenheiten, so dass es auch verständlich ist, dass das Opfer den Drang verspürte, sich um den Papierkram zu kümmern, sobald es die - in diesem Fall böswillige - SMS erhielt.

Fall 6 – Spam-Phishing

Titel	Spam-Phishing
Quelle des Falles	Staatliche Stelle
Zeitraum des Auftretens	im Jahr 2018 aufgetreten
Tags	Regierungsstelle, Identitätsdiebstahl, Social Engineering, E-Mail-Angriff, Phishing
Status	geschlossen durch Änderung der Anmeldedaten
Anwendbarkeit Escape Room	Mit Schwierigkeiten anwendbar: Es handelt sich um eine sehr ausgeklügelte Phishing-Kampagne, so dass es schwierig sein dürfte, bestimmte Elemente zu reproduzieren.

Augen auf Social Engineering:
Die Technik der Social-Engineering-Angriffe besteht in der psychologischen Manipulation von Benutzern, um sie zu Sicherheitsfehlern oder zur Preisgabe sensibler Informationen zu verleiten. In diesem Fall untersuchten die unbekannten Cyber-Kriminellen zunächst die beabsichtigten Opfer, um die für den Angriff erforderlichen Hintergrundinformationen zu sammeln, z. B. über potenzielle Einstiegspunkte und schwache Sicherheitsprotokolle.

Was für ein Angriff war das?

Spam-Phishing

Schwäche/Verwundbarkeit

Menschlicher Fehler - Social Engineering. Die Opfer sind auf einen sehr ausgeklügelten Betrug hereingefallen, der sorgfältig ausgearbeitet und im Laufe der Zeit weiterentwickelt wurde. Wenn Cyberkriminelle Verfahren einführen, um die Opfer zu halten, ist es sehr schwierig, bösartige E-Mails von echten zu unterscheiden. Dies ist eines der Hauptrisiken im Zusammenhang mit Social Engineering, das die Schwächen der Opfer ausnutzt, in diesem Fall eine psychologische Belohnung in Verbindung mit einer Leidenschaft, um sensible Informationen zu erpressen.

Was ist passiert?

- Zum Zeitpunkt des Angriffs wurden die E-Mails der Mitarbeiter dieser Regierungsbehörde auf die gleiche Weise generiert: Vorname + Nachname + Domäne. Die Informationen der Inhaber von E-Mail-Adressen wurden also nicht verschleiert, da sie nicht als sensible Daten betrachtet wurden.
- Dies erleichterte es den Kriminellen, die Identitäten einer Gruppe von Mitarbeitern aufzuspüren. Die Täter begannen, die sozialen Profile - Instagram, Facebook, Twitter, LinkedIn - dieser Mitarbeiter auszuspionieren, und anhand der geposteten Fotos und Videos, der Seiten, denen sie folgten, und der Follower identifizierten sie eine gemeinsame Leidenschaft von etwa 20 Mitarbeitern: Bodybuilding. So begann eine sehr ausgeklügelte Phishing-Kampagne.
- Zunächst starteten die Kriminellen eine Phishing-Testaktion: Sie schickten leere E-Mails an die Opfer, um zu sehen, wer am ehesten in die Falle tappen würde. Anschließend erhielten diese Mitarbeiter eine E-Mail über eine neue Vereinbarung zwischen der Regierungsbehörde und einer bekannten Marke für Trainingsergänzungen, in der diese Marke eine Verkaufskampagne startete. Indem sie ihre Kauf- und Versandinformationen über den Link in der E-Mail eingaben, hätten sie an dieser Verkaufsaktion teilgenommen und die Produkte zu einem sehr günstigen Preis an ihre Haustür geliefert bekommen. Von diesen 20 Mitarbeitern wurden nur zwei betrogen.
- Wenn sie auf den Link klickten, wurden sie auf die - gefälschte - Anmeldeseite der Behörde weitergeleitet, wo sie sich mit ihren Anmeldedaten (Benutzername und Kennwort) anmelden mussten, da es sich um eine Aktion handelte, die ausschließlich für Mitarbeiter dieser Behörde bestimmt war.
- Sobald die Zahlung auf der Website der gefälschten Marke "abgeschlossen" war - auf der sogar eine Kundendienstnummer zur Verfügung stand -, setzten die Kriminellen ein Verfahren in Gang, um das Opfer durch den Versand der gekauften Waren zu halten. Die Kriminellen sorgten dafür, dass der Versand plausibel war: Sie kümmerten sich um jedes Detail, wie die Verpackung, die Etiketten usw.

- Nachdem die beiden Opfer die gekauften Waren erhalten hatten, erzählten sie ihren Kollegen von der angeblichen Echtheit dieser Verkaufsaktion. Auf diese Weise begann der aus der Phishing-Kampagne resultierende bösartige Link unter den Mitarbeitern – auf verschiedenen Ebenen – zu zirkulieren, und innerhalb weniger Tage tappten bis zu 300 Personen in die Falle.

Wie wurde sie wahrgenommen?

Als ein Vorgesetzter erfuhr, was vor sich ging, war ihm sofort bewusst, dass die Mitarbeiter einem Betrug zum Opfer gefallen waren. Er wusste, dass es eine Vereinbarung mit der Marke gab. Die Mitarbeiter gaben nicht nur leichtsinnig ihre persönlichen Daten und Zahlungsinformationen weiter, sondern setzten auch die Behörde, für die sie arbeiten, einem Risiko aus, da diese als Regierung über eine große Anzahl von persönlichen Daten der Bürger verfügt, die zu unzähligen böswilligen Zwecken verwendet werden könnten.

Welche Maßnahmen wurden ergriffen?

- Um dem Betrug Einhalt zu gebieten, wurden alle Konten der Betrugsopfer gesperrt und die Passwörter anschließend geändert.
- Die Regierung ist heute dazu übergegangen, auch die Benutzernamen zu ersetzen.

Was ist das Ergebnis der technischen / organisatorischen / sozialen Abwehrmaßnahmen?

- Das Problem wurde durch die Änderung von Passwörtern und nach und nach auch von Benutzernamen gelöst.
- Heute, vier Jahre nach dem Angriff, sind alle E-Mail-Adressen geändert worden: Es ist nicht mehr möglich, die Identität der Inhaber von E-Mail-Adressen zurückzuverfolgen, da Vor- und Nachname durch einen Code ersetzt worden sind.

5.2 Fälle von Cybersecurity in Deutschland

Fall 1 – Spam-E-Mails

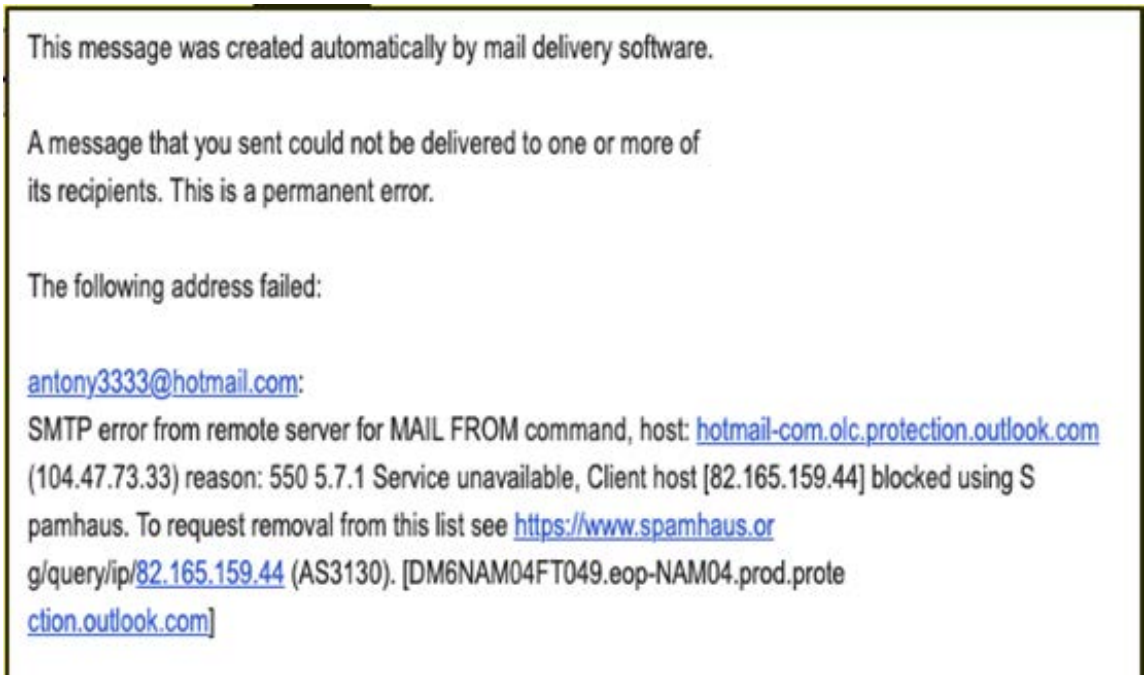
Titel	Spam-E-Mails
Quelle des Falles	Medientechnische Beratung, deutscher/ Bielefelder Mittelstand
Zeitraum des Auftretens	aufgetreten März 2022
Tags	KMU, Identitätsdiebstahl, E-Mail-Attacke, Betrug
Status	geschlossen am 25.3.22 durch Passwortänderung
Anwendbarkeit Escape Room	• Anwendbarkeit und Übertragbarkeit auf das Escape-Room-Modell • Sehr gut anwendbar: Der einfache Fall ist leicht zu verstehen und kann auf ein begrenztes Escape-Room-Modell übertragen werden

Augen auf Identitätsdiebstahl:
Identitätsdiebstahl ist ein Verbrechen, bei dem persönliche oder finanzielle Informationen einer anderen Person erlangt werden, um deren Identität für Betrugszwecke zu nutzen, z. B. für nicht genehmigte Transaktionen oder Einkäufe. Identitätsdiebstahl wird auf viele verschiedene Arten begangen, und die Opfer erleiden in der Regel einen Schaden in Bezug auf ihre Kreditwürdigkeit, ihre Finanzen und ihren Ruf.

Was für ein Angriff war das?
Identitätsdiebstahl

Schwäche/Verwundbarkeit:
Menschlicher Fehler - Passwort zu einfach oder nicht kürzlich geändert.

Was ist passiert?
- Der Täter erlangte offenbar das Passwort für das Konto des Opfers. Von diesem Konto aus verschickte der Cyberkriminelle Spam-E-Mails, vermutlich an eine große Zahl von Adressen, die dem Opfer unbekannt waren.
- Wie aus Abbildung 3 hervorgeht, wurde diese E-Mail vom empfangenden E-Mail-Server aufgrund der Spam-Erkennung blockiert. Es ist davon auszugehen, dass eine große Anzahl von Spam-E-Mails, die automatisch vom Konto des Opfers aus versandt wurden, die vom Angreifer angegebenen Adressen erreichten. Dies ist die primäre Auswirkung des Angriffs.



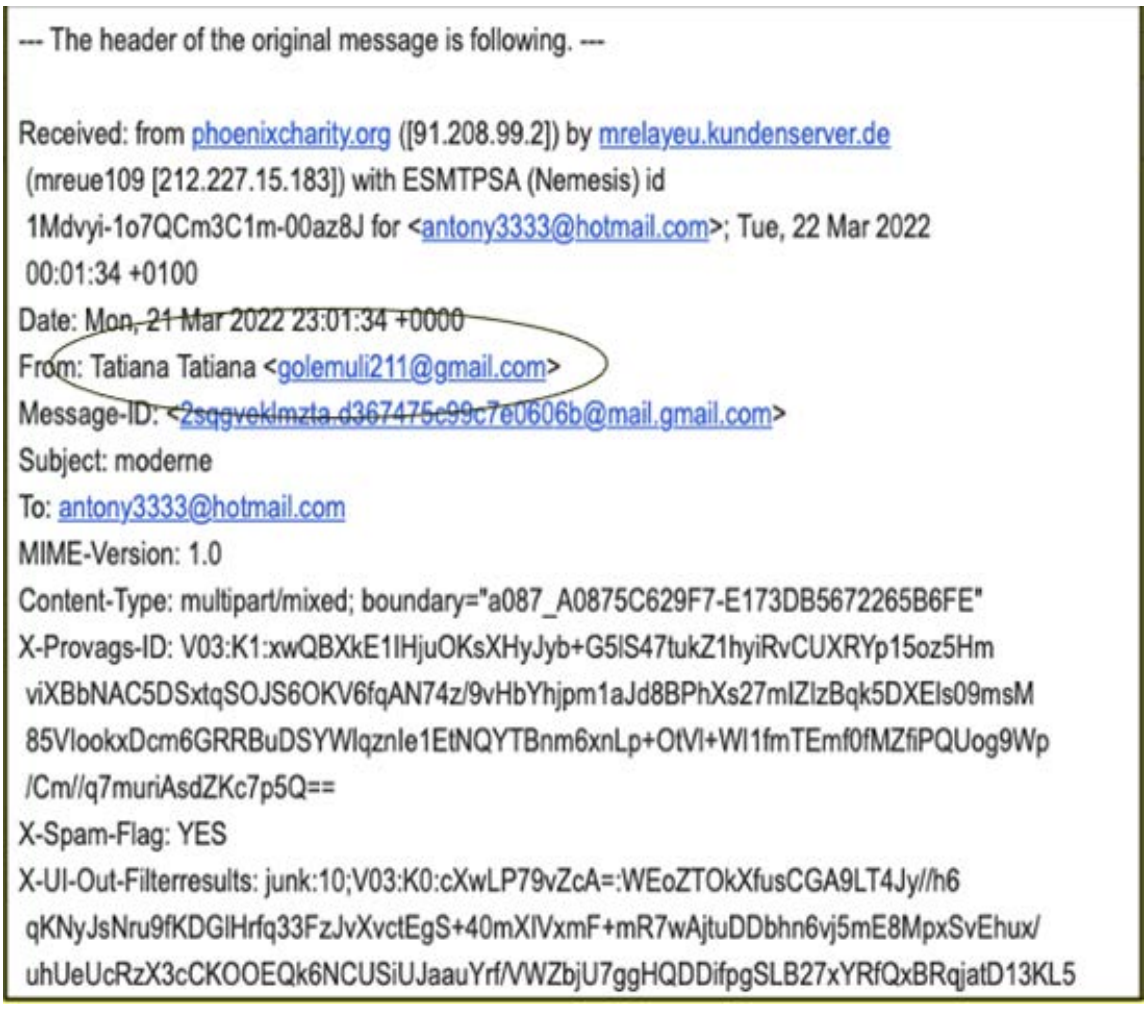
This message was created automatically by mail delivery software.

A message that you sent could not be delivered to one or more of
its recipients. This is a permanent error.

The following address failed:

antony3333@hotmail.com:
SMTP error from remote server for MAIL FROM command, host: hotmail-com.olc.protection.outlook.com
(104.47.73.33) reason: 550 5.7.1 Service unavailable, Client host [82.165.159.44] blocked using S
pamhaus. To request removal from this list see https://www.spamhaus.or
g/query/ip/82.165.159.44 (AS3130). [DM6NAM04FT049.eop-NAM04.prod.prote
ction.outlook.com]

Abbildung 3: Fehlerbenachrichtigungsmail vom empfangenden Mailserver.



--- The header of the original message is following. ---

Received: from phoenixcharity.org ([91.208.99.2]) by mrelayeu.kundenserver.de
(mreue109 [212.227.15.183]) with ESMTPSA (Nemesis) id
1Mdvyi-1o7QCm3C1m-00az8J for <antony3333@hotmail.com>; Tue, 22 Mar 2022
00:01:34 +0100
Date: Mon, 21 Mar 2022 23:01:34 +0000
From: Tatiana Tatiana <golemuli211@gmail.com>
Message-ID: <2sqqveklmzta.d367475c99c7e0606b@mail.gmail.com>
Subject: moderne
To: antony3333@hotmail.com
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="a087_A0875C629F7-E173DB5672265B6FE"
X-Provags-ID: V03:K1:xwQBXkE1lHjuOKsXHyJyb+G5lS47tukZ1hyiRvCUXRYp15oz5Hm
viXBbNAC5DSxtqSOJS6OKV6fqAN74z/9vHbYhjpm1aJd8BPhXs27mlZlzBqk5DXEls09msM
85VlookxDcm6GRRBuDSYWlqznle1EtNQYTBnm6xnLp+OtVl+Wl1fmTEmf0fMZfiPQUog9Wp
/Cm//q7muriAsdZKc7p5Q==
X-Spam-Flag: YES
X-UI-Out-Filterresults: junk:10;V03:K0:cXwLP79vZcA=:WEoZTOkXfusCGA9LT4Jy//h6
qKNyJsNru9fKDGlHrfq33FzJvXvctEgS+40mXlVxmF+mR7wAjtuDDbhn6vj5mE8MpxSvEhux/
uhUeUcRzX3cCKOOEQk6NCUSiUJaauYrf/VWZbjU7ggHQDDifpgSLB27xYRfQxBRqjatD13KL5

Abbildung 4: Kopfzeile der Spam-Mail.

Über die versendeten Inhalte können nur Vermutungen angestellt werden.

- Weitere Nachforschungen[17] ergaben, dass häufig Spam-/Betrugsmails mit der Absenderadresse golemuli211@gmail.com den in Abbildung 4 dargestellten Inhalt verbreiten. Es muss angemerkt werden, dass der Betrüger nicht die Absenderadresse des Opfers verwendet hat.
- Der Schaden scheint sich also auf das Versenden von Spam/Betrug vom Konto des Opfers aus zu beschränken. Es wurde kein Geld vom Opfer verlangt.

Wie wurde sie wahrgenommen?

Der E-Mail-Anbieter des Opfers erkannte offensichtlich den Kontomissbrauch und schickte dem Opfer die folgende Warnung (siehe Abb. 4). Gleichzeitig bemerkte das Opfer des Angriffs, dass E-Mails, die offensichtlich von seinem Konto aus gesendet wurden, von den empfangenden Mailservern zurückgewiesen wurden. Die Anzahl dieser Mails war sehr hoch, etwa 200.

Welche Maßnahmen wurden ergriffen?

Maßnahme: Wechsel zu einem sichereren Passwort

Um dieses Problem zu lösen, wurden die folgenden Kontrollen und Maßnahmen durchgeführt:

- Check 1: Wurde(n) die E-Mail(s) ohne Wissen der Nutzer versendet?
  - Überprüfen Sie ihre Endgeräte (PC, Smartphone oder Tablet) mit einem aktuellen Virenscanner.
  - Aktualisieren Sie die Software auf den Endgeräten der Benutzer und aktivieren Sie automatische Updates.
  - Verwenden Sie die Firewall Ihres Routers, PCs oder Ihre Internet-Sicherheitssoftware.
  - Wenn ein Virus gefunden und erfolgreich entfernt wurde, ändern Sie Ihre Kennwörter.

- Check 2: Hat der Benutzer die E-Mail absichtlich gesendet?
  - Prüfen Sie, ob die von Ihnen verwendete E-Mail-Software richtig konfiguriert ist.
- Sicherstellung der Erreichbarkeit der Empfängeradressen durch regelmäßige Pflege der Mailinglisten der Nutzer.
- Wenn Nutzer Newsletter oder andere Massensendungen versenden, sollten sie die folgenden Standards beachten:
  - Hatte der Absender die Zustimmung des Empfängers (double opt-in)?
  - Der Newsletter enthält einen Link, über den sich der Empfänger mit nur einem Klick abmelden kann (Opt-out)
  - E-Mail-Empfänger, für die der Benutzer eine unzustellbare Nachricht erhält, werden automatisch aus der Adressdatenbank gelöscht (Bounce-Management)

Was ist das Ergebnis der Schutzmaßnahmen?

- In diesem Fall wurde das E-Mail-Passwort vom Opfer innerhalb eines kurzen Zeitraums geändert.
- Die Sperrung wurde vom Provider innerhalb weniger Minuten automatisch aufgehoben.

17 https://www.django-hurtig.com/jagdzentrum/jagd_vorgang_mainstream_id.php?id2=21727

Fall 2 – Installation der Crypto-Miner-Software

Titel	Crypto Miner Software wurde installiert
Quelle des Falles	Nicht genannter Kunde/ Deutschland
Zeitraum des Auftretens	aufgetreten Juni 2019
Tags	SME, Krypto Miner, Krypto Jacking, Betrug
Anwendbarkeit Escape Room	Sehr gut anwendbar: Der einfache Fall ist leicht zu verstehen

Augen auf Krypto-Schürfen:
Das Mining von Kryptowährungen ist ein Prozess, bei dem neue digitale "Münzen" geschaffen werden. Das ist jedoch schon alles, was die Einfachheit ausmacht. Der Prozess der Rückgewinnung dieser Münzen erfordert das Lösen komplexer Rätsel, die Validierung von Kryptowährungstransaktionen in einem Blockchain-Netzwerk und das Hinzufügen zu einem verteilten Hauptbuch, um sie zu lokalisieren.

Was für ein Angriff war das?
Krypto-Schürfer

Schwäche/Verletzlichkeit:
Menschliches Versagen – Das Herunterladen und Installieren von Open-Source-Software aus dem Internet war der Auslöser für diesen Angriff. Sie wurde nicht von "sicheren" oder "offiziellen" Herstellerseiten heruntergeladen.

Was ist passiert?
- Bei einem Kunden wurden infolge eines willkürlichen Software-Downloads durch die Mitarbeiter Krypto-Miner installiert. Als die Krypto-Miner deinstalliert wurden, begann eine Verschlüsselung der Netzwerkstruktur (Server, Clients, Backups, Schattenkopien usw.). Darauf folgte eine Erpressung des Clients.
- Die Mitarbeiter des Kunden hatten lokale Administratorrechte und durften Software auf den Clients installieren. Infolgedessen hatten sich auch Krypto-Miner installiert.
- Die Krypto-Miner begannen sofort nach der Installation zu arbeiten und nutzten die gesamten Client-Ressourcen für das Mining.

Wie wurde sie wahrgenommen?
Die Leistung der Clients wurde immer schlechter. Einfache Prozesse benötigten sehr viel Zeit. Außerdem lag die Auslastung der CPU und des Arbeitsspeichers konstant bei 99 %.

Welche Maßnahmen wurden ergriffen?

- Die Netzstruktur wurde vom Internet abgekoppelt.
- Die Clients und Server wurden aus dem Netzwerk entfernt.
- Die gesamte technische Infrastruktur wurde neu installiert.
  - Einheitlicher Virenschutz, extern gespeicherte Backups, Adminrechte wurden den Benutzern entzogen.
  - Firewall-System wurde installiert.

Was ist das Ergebnis der Schutzmaßnahmen?

- Infolge der durchgeführten Sicherheitsmaßnahmen kam es zu keinem erneuten Befall.
- Bereits heruntergeladene Malware wurde vom Virenschutzsystem entfernt, bevor sie ausgeführt werden konnte.
- Während der Deinstallation startete die Software eine Verschlüsselung der Netzwerkstruktur. Dabei wurden alle im Netzwerk vorhandenen Geräte verschlüsselt.
- Die Backups und Schattenkopien wurden gelöscht und konnten nicht wiederhergestellt werden. Der Kunde wurde vom 01.07.19 auf den 31.12.18 zurückgesetzt.
- Die Daten mussten manuell gepflegt werden. Es gab keine Reaktion auf die Erpressung.
- Die Infrastruktur wurde neu installiert und teilweise aus den vorhandenen alten Backups wiederhergestellt.

Gelernte Lektionen:
Diese Art von Angriff kann sich wiederholen. Sie kann aber durch einen einheitlichen, aktuellen Virenschutz mit Zusatzmodulen wie einem Intercept X oder einer Sandbox verhindert werden. Außerdem können den Nutzern die Admin-Rechte entzogen werden, so dass nicht einfach irgendeine Software installiert werden kann.

Fall 3 – Phishing-Mail/Attacke

Titel	Phishing-Mail/Angriff
Quelle des Falles	Nicht genannter Kunde / Deutschland
Zeitraum des Auftretens	aufgetreten Februar 2022
Tags	KMU, Phishing, Betrug
Status	Der Fall wurde technisch gelöst.
Anwendbarkeit Escape Room	Fall gut anwendbar: Der einfache Fall ist leicht zu verstehen und kann auf ein begrenztes Escape-Room-Modell übertragen werden. Da der Fall ein sehr häufig vorkommender Standardfall ist, ist er für das Modell nicht sehr interessant.

Was für ein Angriff war das?
Phishing

Schwäche/Verwundbarkeit:
Menschliches Versagen – der Benutzername und das Passwort des Kunden für das Online-Banking wurden über den Link in einer Phishing-Mail eingegeben und an den Phishing-Täter übermittelt.

Was ist passiert?
Einem Kunden wurden Phishing-Mails mit aktualisierten Geschäftsbedingungen oder Kostenänderungen zugesandt. Anschließend musste der Online-Banking-Login durchgeführt werden, um die Änderungen einzusehen.

Wie wurde sie wahrgenommen?
Der interne IT-Administrator des meldenden Unternehmens wurde kontaktiert. Er analysierte und prüfte die E-Mail.

Welche Maßnahmen wurden ergriffen?
- Die Mail-Domäne wurde von der Firewall blockiert.
- Allerdings wurden durch diesen Betrug etwa 3000 € auf ein anderes Bankkonto überwiesen. Derzeit steht die Rückerstattung durch die Bank noch aus.

Was ist das Ergebnis der technischen / organisatorischen / sozialen Abwehrmaßnahmen?
- Die Mitarbeiter wurden im Bereich der Sensibilisierung geschult.
- Die Mitarbeiter erhielten ein "Infoblatt" mit Informationen darüber, wie sie Phishing-Mails erkennen können.
- Danach wurden die Phishing-Mails nicht mehr angeklickt und direkt gelöscht.

Gelernte Lektionen:
Diese Art von Angriffen kann sich jederzeit wiederholen. Eine nachhaltige Lösung ist schwer zu implementieren. Offizielle Mail-Domains wie Gmail o.ä. können verwendet werden. Wenn man diese blockiert, kommen unter anderem keine "offiziellen/korrekten" Mails mehr an. Auch die Links werden bei jedem Angriff neu generiert. Hier bietet das Blockieren nur einen temporären Schutz.

Fall 4 – Phishing-Mails/Attacken

Titel	Phishing-Mails zur Erlangung von Mail-Login-Daten
Quelle des Falles	Verwaltung einer Bildungseinrichtung / Deutschland
Zeitraum des Auftretens	aufgetreten März 2022
Tags	KMU, Phishing, Anmeldedaten, Spam
Status	Der Fall wurde erfolgreich bearbeitet und abgeschlossen.
Anwendbarkeit Escape Room	Fall gut anwendbar: Der einfache Fall ist leicht zu verstehen und kann auf ein begrenztes Escape-Room-Modell übertragen werden. Da der Fall ein sehr häufig vorkommender Standardfall ist, ist er für das Modell nicht sehr interessant.

Was für ein Angriff war das?
Phishing

Schwäche/Verwundbarkeit:
Es lag kein Fehlverhalten der Kollegin vor, sie hat sich korrekt verhalten und den Vorfall gemeldet. Der Spam- und Betrugsschutz ließ die Mail in diesem Fall durch, da die Punktzahl für eine Mailabwehr nicht erreicht wurde.

Was ist passiert?
- Die Mitarbeiterin der Bildungseinrichtung erhielt eine Phishing-E-Mail, in der es hieß, ihr E-Mail-Passwort sei abgelaufen und sie solle ein neues Passwort festlegen.
- Der Absender der Mail war der angebliche Provider: Ionos (1&1) Support.

Wie wurde sie wahrgenommen?
- Durch die Wachsamkeit und Informiertheit des Mitarbeiters wurde das Problem bemerkt, und die Kollegen informierten proaktiv den Admin der IT-Abteilung. Die Mitarbeiter waren sich der Tatsache bewusst,

Abbildung 5: Sicherheitshinweis.

dass die verschiedenen Dienstanbieter niemals Mails mit diesem Inhalt versenden würden. Passwörter laufen in der Einrichtung nicht ab.
- Außerdem konnte der Absender bei näherer Betrachtung als nicht legitim identifiziert werden.

Welche Maßnahmen wurden ergriffen?

- Der Kollege leitete die E-Mail an den IT-Administrator weiter.
- Die IT-Abteilung ergriff daraufhin die üblichen Sicherheitsmaßnahmen:
  - Zunächst wurde ein Eintrag in der Mitteilungszentrale formuliert, um alle anderen Kollegen zu warnen, dass zum gegebenen Zeitpunkt Phishing-Angriffe stattgefunden haben.
  - Parallel dazu wurde der Absender blockiert, so dass keine Hintergrundkommunikation stattfinden kann (Blacklist).

Was ist das Ergebnis der Schutzmaßnahmen?

- Da die Opfer und IT-Abteilungen gegen solche Phishing-Angriffe praktisch machtlos sind und keine nachhaltigen Abwehrmechanismen installiert werden können, ohne den Nutzer spürbar einzuschränken, konnten keine weiteren Maßnahmen ergriffen werden.
- Abgesehen von der Arbeitszeit, die in die Klärung des Vorfalls investiert wurde, ist kein Schaden entstanden.

Gelernte Lektionen:
Nach der Auswertung des Vorfalls wurden zusätzliche Präventionskampagnen und Mitarbeiterschulungen geplant, um die Wachsamkeit zu erhöhen.

Fall 5 – Bösartiger Code im E-Mail-Anhang

Titel	Bösartiger Code im E-Mail-Anhang
Quelle des Falles	Universität / Deutschland
Zeitraum des Auftretens	aufgetreten Juni 2016
Tags	SME, Mail, Anhang, Spam, Ransomware
Status	Der Fall wurde erfolgreich bearbeitet und abgeschlossen.
Anwendbarkeit Escape Room	Fall sehr gut einsetzbar: Der einfache, aber lehrreiche Fall ist leicht zu verstehen und kann sehr gut auf ein interessantes Escape-Room-Modell übertragen werden. Darüber hinaus ist es möglich, aus dem Fall ein Szenario für eine lehrreiche und spannende Geschichte zu entwickeln.

Augen auf Locky-Angriff:
Locky ist eine Art von Ransomware. Sie wurde 2016 veröffentlicht, wobei Sicherheitsexperten feststellten, dass die Malware-Autoren diese Ransomware per E-Mail verschickten und zur Zahlung durch eine angehängte Rechnung eines schädlichen Microsoft Word-Dokuments aufforderten, das infektiöse Makros ausführt. Locky Ransomware ist eine Malware, die wichtige Dateien auf Ihrem Computer verschlüsselt und sie damit unzugänglich und unbrauchbar macht. Sie hält sie als "Geisel" gefangen und fordert in der Zwischenzeit eine Lösegeldzahlung im Austausch für die verschlüsselten Dateien.

Was für ein Angriff war das?
Locky-Angriff - Ransomware-Trojaner.

Schwäche/Verwundbarkeit:
Menschlicher Fehler - Öffnen eines unbekannten E-Mail-Anhangs. Der erfolgreiche Angriff wurde durch die Unachtsamkeit des Opfers und die Zero-Day-Variante dieses Trojaners begünstigt.

Was ist passiert?
- Eine E-Mail mit einer Zip-Datei, die Rechnungen enthalten sollte, wurde an ein Teammitglied (das Opfer) gesendet.
- Diese Zip-Datei war verschlüsselt, so dass sie von Antiviren-Systemen nicht überprüft werden konnte.
- Das Passwort für die Zip-Datei stand im Text der E-Mail.
- Das Opfer öffnete die Zip-Datei ohne weitere Überprüfung, entpackte die xlsm-Datei und öffnete sie. Anschließend machte das Opfer seine Mittagspause.
- Der Virenschutz (Kaspersky) - die Zero-Day-Variante dieses Trojaners - und die Mittagspause des Kollegen führten dazu, dass die Anwendung im Hintergrund genügend Zeit hatte, um alle Daten zu kompromittieren.

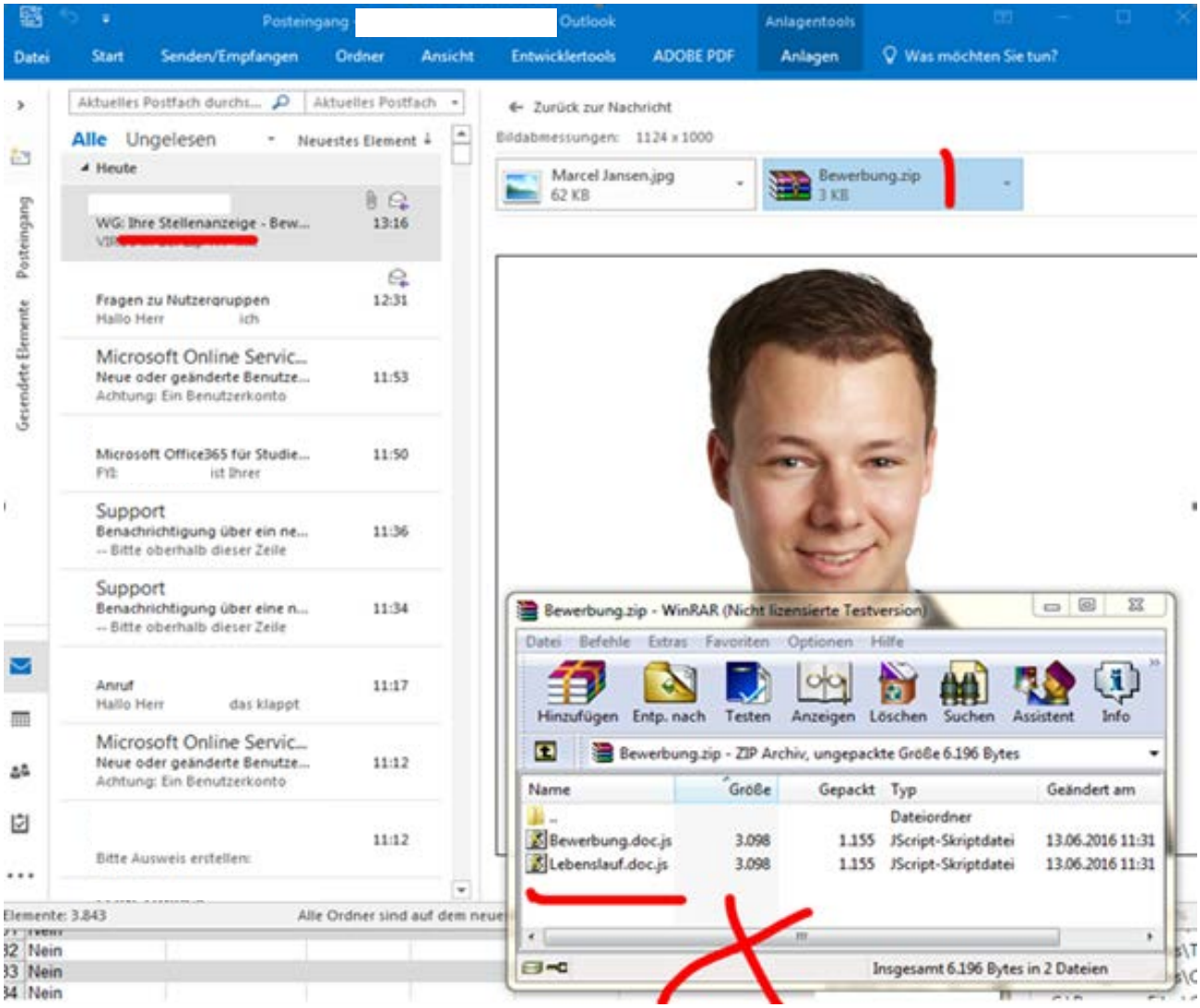


Abbildung 6: Die gefährliche Anlage.

Wie wurde sie wahrgenommen?

- Als das Opfer an seinen Arbeitsplatz zurückkehrte, wunderte es sich über den veränderten Hintergrundbildschirm und informierte die IT-Abteilung.
- Zu diesem Zeitpunkt war etwa eine Stunde vergangen, seit das Opfer auf die angehängte Makro-Excel-Datei geklickt hatte.
- In dem Moment, in dem der Administrator am Computer des Opfers erschien, um in einer Notsituation zu helfen, zog der Administrator sofort das LAN aus und trennte das WLAN.
- Leider war es bereits zu spät, und der Angriff war erfolgreich durchgeführt worden.
- Der Administrator fand eine katastrophale Situation vor: alle Dokumente waren verschlüsselt und nicht mehr verwendbar. Neben den lokalen Dokumenten waren auch alle auf den Netzlaufwerken zugänglichen Dokumente verschlüsselt worden.

Welche Maßnahmen wurden ergriffen?

- Um mit der Entschlüsselung zu beginnen, verlangte der Kriminelle 500 Dollar in Form von Bitcoins.
- Etwa 50 % der Mitarbeiter konnten nicht mehr auf die arbeitsbezogenen Dokumente auf dem Netzlaufwerk zugreifen.
- Der Administrator baute daraufhin den fraglichen Laptop ab. Gleichzeitig wurde im Kundenmanagementsystem (CMS) ein Hinweis auf diesen Vorfall veröffentlicht, damit die telefonische Erreichbarkeit wiederhergestellt werden konnte.
- Die IT-Abteilung sorgte sofort dafür, dass der verursachende Laptop im Netzwerk nicht mehr zugänglich war und keine weiteren Dateien auf dem Netzlaufwerk verschlüsselt wurden.
- Der Laptop wurde vollständig formatiert und Windows neu installiert. Es waren keine lokalen Arbeitsdateien vorhanden.

Was ist das Ergebnis der technischen / organisatorischen / sozialen Abwehrmaßnahmen?

- Die IT-Abteilung spielte in Absprache mit der Geschäftsleitung ein vollständiges Backup des Vortages ein. Dadurch waren alle Vorgänge aller Mitarbeiter aus den letzten 24 Stunden nicht mehr verfügbar. Für einige Mitarbeiter war dies sehr kritisch, aber für die meisten war der Schaden begrenzt.
- Das Opfer erhielt eine spezielle Schulung, um zu verhindern, dass sich ein solcher Fall wiederholt.
- Einen Tag später teilte der damalige Antivirenhersteller mit, dass Locky-Bedrohungen nun ebenfalls erkannt und verhindert werden.

Fall 6 – CEO-Betrug

Titel	CEO-Betrug
Quelle des Falles	Universität / Deutschland
Zeitraum des Auftretens	aufgetreten April 2020
Tags	KMU, Post, Betrug, Spam, Scam
Status	Das Problem besteht nach wie vor. (Zumindest ähnliche Versuche werden immer noch erkannt, aber sie beschränken sich jetzt auf eine begrenzte Anzahl von Beispielen, z. B. Apple-Geschenkkarten).
Anwendbarkeit Escape Room	Fall ist gut anwendbar: Der einfache, aber lehrreiche Fall ist leicht zu verstehen und kann sehr gut auf ein interessantes Escape-Room-Modell übertragen werden. Darüber hinaus ist es möglich, aus dem Fall ein Szenario für eine lehrreiche und spannende Geschichte zu entwickeln.

Augen auf CEO-Betrug:
Der Angreifer gibt sich als Geschäftsführer eines bestimmten Unternehmens aus und versucht, das Opfer dazu zu zwingen, im Namen des echten Geschäftsführers böswillige Handlungen und/oder Betrug durchzuführen.

Was für ein Angriff war das?

CEO-Fraud ist eine sehr gezielte Form des Spear-Phishings, bei der Angreifer potenzielle Opfer und deren Unternehmen online recherchieren und alles, was sie können, von der Website des Unternehmens sowie von Informationen aus sozialen Medien wie LinkedIn, Facebook und Twitter erfahren. In der Regel zielt der Angreifer darauf ab, Sie dazu zu bringen, Geld auf ein Bankkonto zu überweisen, das dem Angreifer gehört, vertrauliche Personalinformationen zu übermitteln oder andere sensible Informationen preiszugeben.

Schwäche/Verwundbarkeit:

- Es handelt sich um einen CEO-Betrug. Der Absender behauptet, zur Geschäftsleitung zu gehören, mit der Absicht, einen Betrug durchzuführen.
- Der Spam-/Betrugsschutz seitens des Mail-Providers hat versagt oder "Betrug" signalisiert.
- Der Mitarbeiter war nicht geschult, um nicht legitimierte Anfragen sofort zu erkennen. Der Mitarbeiter war auch sehr neu in der Firma und hatte aufgrund von Covid19 wenig Kontakt zu anderen Kollegen.

Was ist passiert?

- Eine E-Mail, angeblich von der Geschäftsleitung, erreicht die Kollegen: Eine Geldüberweisung ins Ausland wurde angefordert.
- Es handelt sich dabei nicht um eine automatisierte Mail; die kontaktierte Person hätte diese Übermittlung selbst veranlassen können.
- Da die echte Mailadresse des Angreifers für den Empfänger nur schwer zu erkennen ist, hat der Nutzer dies nicht wirklich bemerkt.

Wie wurde sie wahrgenommen?

- Da der Geldtransfer bestimmten Regeln und einem Kontrollmechanismus innerhalb der Organisation folgt, konnte die Rechtmäßigkeit des Transfers nicht bestätigt werden. Es wurde schnell klar, dass es sich um einen Betrug handelte.
- Wäre der Nutzer direkt mit der Maus über die Mailadresse gefahren, hätte er schnell gemerkt, dass es sich um einen Betrugsversuch handelt.

Welche Maßnahmen wurden ergriffen?

- Der Angriff wurde durch die Sperrung des E-Mail-Kontos des Absenders (Gmail-Konto des Angreifers) durchgeführt.
- Der Fall wurde der Polizei gemeldet, aber der Täter konnte nicht ermittelt werden.

Was ist das Ergebnis der Schutzmaßnahmen?

Es ist nicht möglich, sich nachhaltig zu schützen, ohne den Postversand zu stark einzuschränken, daher wird der proaktive Schutz weiter verstärkt.

Fall 7 – Backdoor in Software - Spionageangriff

Titel	Backdoor in Software - Spionageangriff
Quelle des Falles	Innenministerium NRW/ Düsseldorf/Deutschland
Zeitraum des Auftretens	Unbekannt.
Tags	Spionageangriff, Hintertür
Status	Aufgelöst
Anwendbarkeit Escape Room	Fall sehr gut einsetzbar: Der interessante Fall ist leicht nachvollziehbar und lässt sich sehr gut auf ein interessantes Escape-Room-Modell übertragen. Darüber hinaus ist es möglich, aus dem Fall ein Szenario für eine lehrreiche und spannende Geschichte zu entwickeln.

Augen auf Spionage Attacken:
Der Diebstahl von Forschungsergebnissen, Produktentwicklungsinformationen, Bilanzzahlen und Kundendaten schadet den betroffenen Unternehmen nachhaltig: Ausländische Konkurrenten erhalten die Daten unentgeltlich. Ein hart erkämpfter Wettbewerbsvorteil kann verloren gehen, so dass der Produktabsatz sinkt. Ausländische Nachrichtendienste verfügen über ausgezeichnete IT-Kenntnisse und verbergen ihren Zugang. Die Entdeckung eines Angriffs erfolgt oft erst, wenn ein externer Hinweisgeber das Unternehmen auf den Angriff aufmerksam macht.

Was für ein Angriff war das?

Spionageangriff, Hintertür

Schwäche/Verwundbarkeit:

Die Fremdsoftware hätte nicht ungeprüft im Firmennetz eingesetzt werden dürfen. Stattdessen hätte mit einem Sicherheitskonzept geprüft werden müssen, ob die Software isoliert eingesetzt werden kann.

Was ist passiert?

- Unternehmen mit Geschäftsbeziehungen ins Ausland sind oft verpflichtet, bestimmte Software zu verwenden, z. B. für die Bearbeitung von Steuerpflichten.
- Eine spezielle Backdoor-Software wurde auf verschiedenen Computern im weltweit vernetzten Unternehmen des Opfers installiert.
- Über eine versteckte Backdoor konnte ein Angreifer auf Dokumente im Netzwerk des Opfers zugreifen.

Wie wurde sie wahrgenommen?

Im Anschluss an die Installation wurde bekannt, dass die vorgeschriebene Software eine Hintertür für den ausländischen Geheimdienst enthält.

Welche Maßnahmen wurden ergriffen?

Das System wurde komplett neu installiert und die Hintertür wurde geschlossen.

Was ist das Ergebnis der Schutzmaßnahmen?

Weitere Anschläge wurden verhindert.

Fall 8 – Erweitertes Social Engineering - Spionageangriff

Titel	Erweitertes Social Engineering - Spionageangriff
Quelle des Falles	Innenministerium NRW/ Düsseldorf/Deutschland
Zeitraum des Auftretens	Unbekannt.
Tags	Spionageangriff, Social Engineering
Status	Aufgelöst
Anwendbarkeit Escape Room	Fall sehr gut und anwendbar: Der interessante Fall ist leicht zu verstehen und lässt sich sehr gut auf ein interessantes Escape-Room-Modell übertragen. Darüber hinaus ist es möglich, aus dem Fall ein Szenario für eine lehrreiche und spannende Geschichte zu entwickeln.

Was für ein Angriff war das?

Spionageangriff

Schwäche/Verwundbarkeit:

Die Angreifer verstehen es geschickt, bei den Opfern die Angst zu schüren, dass sie ein gutes Angebot verpassen könnten. Außerdem wird durch den telefonischen Kontakt das Misstrauen gegenüber dem Angreifer verringert. Trotzdem hätte das bösartige Dokument nicht im Firmennetz geöffnet werden dürfen. Einmal mehr wird die "menschliche Schwäche" ausgenutzt.

Was ist passiert?

- In vielen High-Tech-Bereichen ist es üblich, dass Personalvermittler mit Angeboten für einen Stellenwechsel an die Betroffenen herantreten.
- Als ein Angestellter eines bekannten Unternehmens auf seinem Handy einen Anruf von einem Headhunter erhält, scheint dies nichts Ungewöhnliches zu sein. Nach einem kurzen Gespräch kündigt der vermeintliche Agent an, dass er ein lukratives Jobangebot weiterleiten wird. Kurze Zeit später trifft das Dokument im WhatsApp-Account des Mitarbeiters ein. Als er versucht, es auf seinem Handy zu öffnen, bricht der Vorgang mit einer Fehlermeldung ab.
- Am nächsten Tag kontaktiert der Headhunter den Arbeitnehmer erneut und verspricht ihm außergewöhnliche Verdienstmöglichkeiten und attraktive Arbeitsbedingungen. Eine Rückmeldung über das weitere Interesse an dem unterbreiteten Angebot muss jedoch sofort erfolgen. Kurzerhand überträgt der Mitarbeiter das bei der Präsentation erhaltene Dokument auf sein geschäftliches E-Mail-Konto. Nach einer kurzen Bestätigung, eine spezielle Formatvorlage zu verwenden, kann er die Datei auf seinem Firmencomputer öffnen. Da das Angebot nicht seinen Vorstellungen entspricht, sagt er den Auftrag beim Headhunter ab. Danach ist der Vorgang vergessen.
- Später stellte sich heraus, dass durch das Öffnen des Dokuments ein Fernzugriff auf den Firmen-PC des Mitarbeiters hergestellt wurde. Dieser Zugang ermöglichte es den Angreifern, sich weiter im Firmennetz auszubreiten und sensible Daten abzugreifen. Der Datendiebstahl wurde erst bemerkt, als die Angreifer schon längst verschwunden waren.

Wie wurde sie wahrgenommen?

Keine weiteren Informationen, da der Fall vom Innenministerium NRW nicht bekannt gegeben wird.

Welche Maßnahmen wurden ergriffen?

Keine weiteren Informationen, da der Fall vom Innenministerium NRW nicht bekannt gegeben wird.

Was ist das Ergebnis der Schutzmaßnahmen?

Keine weiteren Informationen, da der Fall vom Innenministerium NRW nicht bekannt gegeben wird.

Fall 9 – Phishing-Mails

Titel	Phishing-Mails
Quelle des Falles	IT-Nachrichtenunternehmen, Deutschland
Zeitraum des Auftretens	Aufgetreten Mai 2019
Tags	Unternehmen, Phishing, E-Mail-Angriff, Ransomware
Status	Der Status dieses Falls ist: Er wurde innerhalb weniger Wochen nach Auftreten des Problems abgeschlossen, indem ein neues Netzwerk eingerichtet und alle während des Angriffs mit dem Netzwerk verbundenen Computer ersetzt wurden.
Anwendbarkeit Escape Room	Sehr gut anwendbar: Emotet und Trojaner sind weithin bekannt, ebenso wie Phishing.

Augen auf Phishing-Angriffen:
Wir haben Phishing-Angriffe bereits beschrieben, aber es ist wichtig zu wissen, dass sich Phishing-Angriffe im Laufe der Jahre angepasst haben und immer "besser" und raffinierter werden. Es ist daher wichtig, sich über die neuesten Phishing-Methoden auf dem Laufenden zu halten.

Was für ein Angriff war das?
Phishing-Angriff

Schwäche/Verwundbarkeit:
Der Mitarbeiter aktivierte Makros für die infizierte Datei.

Was ist passiert?
- Ein Mitarbeiter öffnete eine E-Mail von einem gefälschten Absender, der sich als Geschäftspartner ausgab. Die E-Mail enthielt ein infiziertes Word-Dokument.
- Als der Mitarbeiter diese Datei öffnete, erschien eine Fehlermeldung, die ihn aufforderte, die Bearbeitung zu "aktivieren".
- Der Mitarbeiter klickte auf diese Nachricht, woraufhin Emotet sein System infizierte und begann, sich im Netzwerk zu verbreiten.

Wie wurde sie wahrgenommen?
Es wurden mehrere Infektionen festgestellt, und es wurden mehrere infizierte Computer im gesamten Netzwerk gefunden.

Welche Maßnahmen wurden ergriffen?
- Von verschiedenen Computern aus wurden Verbindungen nach außen hergestellt.
- Der Virus wurde mit Avira und Windows Defender entfernt.

- Anschließend versuchten die Administratoren zu verhindern, dass die Malware mit der Emotet-Infrastruktur kommuniziert. Da dies nicht wie vorgesehen funktionierte, wurde das gesamte Netzwerk vom Internet getrennt.
- Es wurden externe Dienstleister und mehrere IT-Forensik-Unternehmen kontaktiert.

Was ist das Ergebnis der Schutzmaßnahmen?

- Das gesamte Intranet wurde wiederhergestellt und alle Computer, die während des Angriffs mit dem Intranet verbunden waren, wurden ersetzt.
- Das Sicherheitskonzept wurde überarbeitet, um diesen Fall in Zukunft zu verhindern.

Fall 10 – Erpresser-Phishing-Mail

Titel	Erpresser-Phishing-Mail
Quelle des Falles	Elektrogroßhändler (Deutschland)
Zeitraum des Auftretens	Aufgetreten im Februar 2020
Tags	Unternehmen, Phishing, E-Mail-Angriff, KMU, Ransomware
Status	Innerhalb von drei Wochen nach Auftreten des Problems durch Zahlung des Lösegelds geschlossen.
Anwendbarkeit Escape Room	Sehr gut anwendbar: Fehlende Backups sind ein großes Problem, und der Verlust von Daten ohne ein funktionierendes Backup ist katastrophal.

Augen auf Backups:
Eine Sicherungskopie ist eine Kopie von Daten, die getrennt von den Originaldaten erstellt und gespeichert wird. Diese Kopie kann verwendet werden, um die Originaldaten wiederherzustellen, falls sie verloren gehen oder beschädigt werden. Es wird dringend empfohlen, in einem Unternehmen regelmäßig Sicherungskopien zu erstellen und zu testen.

Was für ein Angriff war das?

Phishing-Angriff

Schwäche/Verwundbarkeit:

Die infizierte E-Mail wurde versehentlich von einem Mitarbeiter geöffnet. Die Ransomware verschlüsselte alle Dateien. Ein fahrlässiges Öffnen von verdächtigen E-Mails und Anhängen führte zu dem erfolgreichen Angriff. Außerdem hatte das Unternehmen keine regelmäßige Backup-Strategie. Aufgrund der fehlenden Backup-Kontrollen war das Unternehmen gezwungen, das Lösegeld zu zahlen.

Was ist passiert?

- Ein Mitarbeiter öffnete einen infizierten E-Mail-Anhang. Alle Anzeigen waren weiß und zeigten eine E-Mail-Adresse an. Der Malware-Stamm Emoted infizierte alle Computer und verschlüsselte somit alle Dateien in Reichweite.

- Ein externer Dienstleister, der mit der Erstellung der Backups betraut war, hatte diese noch nicht erstellt. Es war keine aktuelle Sicherung verfügbar, und die einzigen vorhandenen Sicherungen waren zu alt, um damit zu arbeiten.
- Niemand überwachte die Backups und hatte das Datum der letzten Backups überprüft. Auch die Kommunikation mit dem externen Dienstleister verlief unregelmäßig.

Zusätzliche Informationen: Makros werden häufig in Office-Anwendungen wie Word, Excel und PowerPoint verwendet. Diese Makros werden als Teil der Dokumentdatei gespeichert und sind in einer Programmiersprache namens VBA (Visual Basic for Applications) geschrieben. Makros können dazu verwendet werden, ein System mit Malware zu infizieren.

Wie wurde sie wahrgenommen?

Die Dateien waren schnell verschlüsselt, und das System war unbrauchbar.

Welche Maßnahmen wurden ergriffen?

- Das Unternehmen wandte sich an die Polizei und an den Erpresser.
- Der Erpresser forderte 21 Bitcoins. Ohne ein funktionierendes Backup war die Existenz des Unternehmens gefährdet. Daher wurde das Lösegeld in Höhe von 120.000 € gezahlt, und alle Systeme wurden entschlüsselt.
- Kommunikation per Post und drei Wochen lang keine digitale Rechnungsstellung, was zu enormen finanziellen Verlusten führte.

Zusätzliche Informationen: Nicht jedes Unternehmen, das das Lösegeld bezahlt, erhält seine Dateien entschlüsselt zurück. Selbst wenn sie ihre Dateien zurückerhalten, ist es notwendig, alle Dateien auf versteckte Malware zu untersuchen.

Was ist das Ergebnis der Schutzmaßnahmen?

- Das E-Mail-System wurde dann auf eine Cloud-Lösung von Microsoft umgestellt.
- Externe Backups werden jetzt wöchentlich erstellt.
- Regelmäßige Backups und Sicherheitspläne wurden aktiviert.
- Cyber-Sicherheitsschulungen

Fall 11 – Phishing-Mail mit Malware

Titel	Phishing-Mail mit Malware
Quelle des Falles	Unternehmen für Maschinensicherheit (Deutschland)
Zeitraum des Auftretens	Aufgetreten Mai 2020
Tags	Unternehmen, Phishing, E-Mail-Angriff, Ransomware
Status	Innerhalb von zwei Wochen nach Abschaltung des Intranets geschlossen.
Anwendbarkeit Escape Room	Hochgradig zutreffend: E-Mails sind gefährlich, Hinweise von Behörden müssen ernst genommen und überprüft werden.

Augen auf Malware:
Malware, die Abkürzung für bösartige Software, ist jede Software, die darauf abzielt, ein Computersystem oder ein Netzwerk zu schädigen oder auszunutzen. Es gibt verschiedene Arten von Malware, darunter Viren, Würmer, Trojanische Pferde, Ransomware und Spyware. Sie ist oft an andere Software oder Links angehängt und darin versteckt.

Was für ein Angriff war das?
Phishing-Angriff

Schwäche/Verwundbarkeit:
Fahrlässiges Öffnen eines infizierten E-Mail-Anhangs. Die Mitarbeiter waren nicht ausreichend geschult, um eine verdächtige E-Mail zu erkennen.

Was ist passiert?
E-Mail mit Malware wurde geöffnet.

Wie wurde sie wahrgenommen?
- Das Unternehmen wurde von einer Behörde (Landeskriminalamt) über einen drohenden Cyberangriff mittels infizierter Mails informiert.
- Das Unternehmen prüfte diesen Anruf und beschloss, sein Netz sieben Minuten nach dem Anruf abzuschalten.

Welche Maßnahmen wurden ergriffen?
- Unterbrechung des Netzes.
- Untersuchung und Desinfektion aller Systeme des Netzwerks. Nach der Unterbrechung der Verbindung wurde die Malware identifiziert. Die Produktion kam zum Stillstand.
- Jeder Computer musste einzeln desinfiziert werden.
- Der Ersatzserver ermöglichte die E-Mail-Kommunikation.

Weitere Informationen: Die individuelle Desinfektion jedes Computers ist für das Unternehmen sehr zeit- und kostenaufwendig. Der Angriff hätte durch eine entsprechende Schulung verhindert werden können.

Was ist das Ergebnis der Schutzmaßnahmen?
Zwei Wochen später waren das IT-System und die Produktion wieder in Betrieb.

Fall 12 – Ransomware und Phishing

Titel	Phishing-Mail mit Malware
Quelle des Falles	Unternehmen für Maschinensicherheit (Deutschland)
Zeitraum des Auftretens	Aufgetreten Mai 2020
Tags	Unternehmen, Phishing, E-Mail-Angriff, Ransomware
Status	Innerhalb von zwei Wochen nach Abschaltung des Intranets geschlossen.
Anwendbarkeit Escape Room	Hochgradig zutreffend: E-Mails sind gefährlich, Hinweise von Behörden müssen ernst genommen und überprüft werden.

Augen auf DeepBlueMagic:
DeepBlueMagic stammt offenbar aus China. Wie mehrere Ransomware-Stämme in der Vergangenheit verschlüsselt er Dateien mit gängigen Verschlüsselungstools wie Bitlocker und BestCrypt, denen Benutzer oft vertrauen und die sie selbst zur Verschlüsselung verwenden.

Was für ein Angriff war das?
Malware "DeepBlueMagic" über Phishing-Mail installiert.

Schwäche/Verwundbarkeit:
Fahrlässiges Öffnen eines infizierten E-Mail-Anhangs. Die Mitarbeiter waren nicht ausreichend geschult, um eine verdächtige E-Mail zu erkennen.

Was ist passiert?
- Provider für öffentliche Behörden wurden angegriffen. Ein infektiöser E-Mail-Anhang mit Malware wurde geöffnet.
- Es wurden keine persönlichen Daten gestohlen.

Wie wurde sie wahrgenommen?
Die Benutzer erhielten E-Mails von den Cyber-Kriminellen, dass ihre Dateien verschlüsselt und nicht nutzbar seien.

Welche Maßnahmen wurden ergriffen?
- Das regionale Verwaltungsbüro musste geschlossen werden.
- Alle Systeme wurden abgeschaltet.
- Zusätzlich zu den Hauptsystemen mussten 4000 Endgeräte auf Schadsoftware gescannt werden.
- Die Sicherungskopien wurden wiederhergestellt, aber die Wiederherstellung ist noch im Gange.
- Es wurde kein Lösegeld gezahlt.

Zusätzliche Informationen: Dieses Beispiel zeigt, wie wichtig ein funktionierendes Backup-System ist. Selbst nach dem Angriff konnten sie die Daten wiederherstellen, ohne das Lösegeld zu bezahlen. Denken Sie daran: kein Backup - kein Mitleid.

Was ist das Ergebnis der Schutzmaßnahmen?

Bis Ende 2021 waren 95 % aller Daten wiederhergestellt worden.

Fall 13 – Schadsoftware

Titel	Malware
Quelle des Falles	Investment Start-up (Deutschland)
Zeitraum des Auftretens	Aufgetreten Oktober 2021
Tags	Unternehmen, KMU, Ransomware, Social Engineering
Status	Nach einigen Tagen geschlossen, indem die ausgenutzte Sicherheitslücke geschlossen wurde.
Anwendbarkeit Escape Room	Mit Schwierigkeiten anwendbar: Das Ausnutzen von Schwachstellen erfordert ein gewisses Maß an Wissen oder sie müssen sehr leicht zu entdecken sein. Dennoch erfordern sie ein tieferes Verständnis der IT

Augen auf Social Engineering:
Unter Social Engineering versteht man den Einsatz psychologischer Manipulation, um Einzelpersonen oder Gruppen dazu zu bringen, sensible Informationen preiszugeben oder Handlungen vorzunehmen, die ihnen oder ihrer Organisation schaden könnten. Dies kann Taktiken wie Phishing, Vishing (Voice Phishing) und Manipulation am Telefon umfassen. Das Ziel ist immer dasselbe: Menschen dazu zu verleiten, vertrauliche Informationen oder Zugang zu Systemen oder Netzwerken preiszugeben.

Was für ein Angriff war das?

Ransomware-Angriff unterstützt durch Social-Engineering-Anrufe.

Schwäche/Verwundbarkeit:

Gestohlene Daten wurden verwendet, um Social-Engineering-Anrufe zu unterstützen und glaubwürdig zu machen.

Was ist passiert?

- Phishing-Angriffe, die durch Social-Engineering-Anrufe bei den Kunden unterstützt wurden.
- Die Schwachstelle im IT-System wurde nicht rechtzeitig gefunden.
- Eine Sicherheitslücke im System wurde ausgenutzt, um Kundendaten auszuspähen.

Wie wurde sie wahrgenommen?

Bei einer Überprüfung des Systems konnte das Sicherheitsleck bzw. der Angriff schnell lokalisiert werden.

Welche Maßnahmen wurden ergriffen?

- Die Kunden wurden drei Tage später informiert.
- Die Behörden wurden informiert.
- Die Sicherheitslücke wurde geschlossen.

Zusätzliche Informationen:

Wenn Sie einen Benutzer haben, der ein Passwort ändern möchte, empfiehlt es sich, dass die zuständige IT-Abteilung Anforderungen bezüglich sicherer Passwörter veröffentlicht.

Was ist das Ergebnis der Schutzmaßnahmen?

Nachdem die Sicherheitslücke geschlossen war, wurden die Kunden benachrichtigt und aufgefordert, ihre Passwörter zu ändern.

Fall 14 – Malware im Unternehmen

Titel	Malware im Unternehmen
Quelle des Falles	Hersteller von Industriemaschinen (Deutschland)
Zeitraum des Auftretens	Aufgetreten Juli 2021
Tags	Unternehmen
Status	Erholte sich nach einigen Monaten.
Anwendbarkeit Escape Room	Mit Schwierigkeiten anwendbar: Der Fall war sehr aufwändig und keineswegs ein Fehler des Unternehmens - Lektion: Egal wie gut Ihre Sicherheit ist, es kann immer einen Angriff geben.

Augen auf Spoof-Mails:

Eine Spoof-Mail ist eine gefälschte Mail, bei der die E-Mail-Adresse des Absenders und andere Teile des E-Mail-Headers so verändert wurden, dass es so aussieht, als stamme die E-Mail von einer anderen Quelle. Dies wird häufig bei Phishing-Betrügereien und anderen Formen des Betrugs verwendet, da es die E-Mail für den Empfänger legitimer erscheinen lassen kann.

Was für ein Angriff war das?

Ausgeklügelter und von langer Hand geplanter Angriff, bei dem ein Dienstleister aus dem Ausland über eine Phishing-Mail und eine gefälschte Website in das Unternehmen eindringt.

Schwäche/Verwundbarkeit:

FDer Dienstleister wurde als Schwachstelle ausgenutzt - obwohl die IT-Sicherheit und die Mitarbeiter des Unternehmens gut vorbereitet waren.

Was ist passiert?

Die Hacker schickten eine gefälschte E-Mail an einen Dienstanbieter im Ausland. Die Mail war mit einer perfekt gefälschten Website verlinkt, so dass der Dienstanbieter den Betrug nicht erkennen konnte.

Wie wurde sie wahrgenommen?

Das System wurde komplett heruntergefahren / unbrauchbar, und alle Dateien wurden verschlüsselt.

Welche Maßnahmen wurden ergriffen?

- Alle Systeme wurden abgeschaltet.
- Alle Geschäftsprozesse wurden gestoppt.
- Erpressungsversuch mit der Conti-Gruppe.
- Für die Wiederherstellung der Systeme wurde ein externer Anbieter von Cybersicherheitslösungen engagiert.

Zusätzliche Informationen: Auch wenn ein Sicherheitssystem gut funktioniert und das Personal entsprechend geschult ist, ist es immer möglich, gehackt zu werden. Leider gibt es keine 100%ige Sicherheit vor Angriffen.

Was ist das Ergebnis der Schutzmaßnahmen?

- Eine Taskforce wurde gegründet. Einrichtung neuer Kommunikationskanäle mit täglichen Nachrichten.
- Die Behörden wurden informiert.
- Verschiedene Geschäftsbereiche wurden nach Prioritäten geordnet.
- Die Infrastruktur wurde neu aufgebaut, externe IT-Beratung und Unterstützung wurden hinzugezogen.
- Die Backups wurden wiederhergestellt und die Wiederherstellung wurde in drei Kategorien eingeteilt: rot (noch infiziert), orange (in Quarantäne) und grün (saubere Daten).

5.3 Fälle von Cybersicherheit in Portugal

Fall 1 – Denial of Service bei Kommunikationsdiensten

Titel	Denial of Service bei Kommunikationsdiensten
Quelle des Falles	Wikipedia[18], Diário de Notícias[19]
Zeitraum des Auftretens	Aufgetreten im Februar 2021
Tags	Unternehmen, Telekommunikation
Status	Der Status dieses Falles ist abgeschlossen.
Anwendbarkeit Escape Room	Der Fall könnte auf das Escape-Room-Modell übertragen werden, da er die Bedeutung der Cybersicherheit für die Gesellschaft zeigt. Allerdings gab das Unternehmen nicht genügend Informationen preis, um ein Szenario für das Spiel zu erstellen.

14 https://pt.wikipedia.org/wiki/Ciberataque_%C3%A0_Vodafone_Portugal
15 https://www.dn.pt/dinheiro/fraude-marca-continente-alvo-de-phishing-11487091.html

Augen auf Identitätsdiebstahl:
Identitätsdiebstahl ist ein Verbrechen, bei dem persönliche oder finanzielle Informationen einer anderen Person erlangt werden, um deren Identität für Betrugszwecke zu nutzen, z. B. für nicht genehmigte Transaktionen oder Einkäufe. Identitätsdiebstahl wird auf viele verschiedene Arten begangen, und die Opfer erleiden in der Regel einen Schaden in Bezug auf Ihre Kreditwürdigkeit, ihre Finanzen und ihren Ruf.

Was für ein Angriff war das?

Das Unternehmen und die Polizei gaben nicht viele Informationen preis. Es wird vermutet, dass eine hochentwickelte Gruppe von Hackern den Angriff durchgeführt hat, indem sie einige Sicherheitslücken in einer nicht aktualisierten Software ausnutzte, aber der verwendete Exploit wurde nicht bekannt gegeben. Mit dem Angriff sollte sichergestellt werden, dass das Unternehmen seine Kommunikationsdienste nicht anbieten kann.

Schwäche/Verwundbarkeit:

Die Schwachstellen waren darauf zurückzuführen, dass die gesamte Software zur Verwaltung der Kommunikationsdienste nicht aktualisiert wurde. Es ist unklar, ob es auch eine interne Zusammenarbeit gab.

Was ist passiert?

Die Hacker nutzten die Software-Schwachstelle aus, um sich Zugang zu den Kommunikationsservern und -systemen zu verschaffen und die Kommunikation zu stören.

Wie wurde sie wahrgenommen?

- Mangel an mobilen Daten im 3G- und 4G-Netz.
- Fehlende Dienste für SMS-, TV- und Festnetz-Internet-Kunden.
- Fehlender Sprachdienst.
- Die 112 (Notrufnummer) konnte nicht erreicht werden.
- SIBS [Eigentümer der Marke Multibanco] ist ein Kunde von Vodafone. Ihr Geldautomatennetz wurde über das Vodafone-Netz unterstützt. Einige der Geldautomaten waren bis etwa Mitternacht nicht verfügbar, da sie über ein Verbindungsnetz zum mobilen Datennetz verfügen.
- Die Geschäfte konnten ihre Produkte nicht online verkaufen, da die Verbindungen zum wichtigsten Bankbetreiber nicht funktionierten.
- Die Kunden konnten die Geldautomaten nicht benutzen.
- Die Kunden konnten in den Geschäften nicht mit Karte bezahlen.

Welche Maßnahmen wurden ergriffen?

Die Notruf- und Gesundheitsdienste wurden zu anderen Kommunikationsunternehmen umgeleitet. Das Unternehmen musste alle Systeme anhalten und dann auf ältere Kommunikationssysteme zurückgreifen. Dann musste es nach und nach alle betroffenen Systeme überprüfen und neu starten. Dies dauerte etwa zwei Wochen.

Was ist das Ergebnis der Schutzmaßnahmen?

Dank der neuen Sicherheitsmaßnahmen sind die Dienste seit dem Vorfall nicht mehr angegriffen worden.

Fehler und Reaktion:

Dieser Einbruch bei Vodafone ist auf die Arbeit von Hackern zurückzuführen, die eine Software-Schwachstelle ausnutzten. Die Menschen waren sehr verärgert, und einige gerieten in Panik, weil sie andere Menschen oder Notrufnummern wie 911 nicht erreichen konnten, einige Unternehmen verloren viel Geld, und die Menschen hatten Angst, dass die Hacker Zugang zu privaten Informationen hatten. Der CEO von Vodafone versicherte jedoch, dass es keinen Zugriff auf private Daten gab. Das Unternehmen hat seitdem die Sicherheitsmaßnahmen verstärkt.

Fall 2 – Phishing bei Einzelhandelskunden

Titel	Phishing bei Einzelhandelskunden
Quelle des Falles	Tageszeitung "Diário de Notícias[20]
Zeitraum des Auftretens	Aufgetreten November 2019
Tags	Unternehmen
Status	Der Status dieses Falles ist abgeschlossen.
Anwendbarkeit Escape Room	Leicht übertragbar auf das Escape Room Modell

Was für ein Angriff war das?
Phishing-Angriff auf Kunden eines großen Einzelhandelsunternehmens.

Schwäche/Verwundbarkeit:
Der Social-Engineering-Ansatz war sehr gut gemacht und nutzte die ahnungslosen Kunden aus.

Was ist passiert?
Die Leute erhielten gefälschte SMS von jemandem, der sich als Mitarbeiter des Einzelhandelsgeschäfts Continente ausgab und nach persönlichen Daten fragte. Einige Personen glaubten den Nachrichten und gaben ihre persönlichen Daten an die Hacker weiter.

Wie wurde sie wahrgenommen?
Die Leute begannen zu sehen, dass Artikel mit ihrer Einzelhandelskarte und ihrem Konto gekauft wurden.

Welche Maßnahmen wurden ergriffen?
Die Kunden wurden über den Angriff informiert und gewarnt. Betroffene Kunden erhielten neue Karten.

Was ist das Ergebnis der Schutzmaßnahmen?
Durch die Informationskampagne konnte verhindert werden, dass eine große Zahl von Kunden betroffen war.

Fehler und Reaktion:
Die Kunden des Einzelhandelsunternehmens (Continente) wurden Opfer von Phishing und haben den Wahrheitsgehalt der Informationen in den E-Mails nicht überprüft.

20 https://www.dn.pt/dinheiro/fraude-marca-continente-alvo-de-phishing-11487091.html

Fall 3 – Gestohlene Daten von öffentlichen Einrichtungen

Titel	Von öffentlichen Einrichtungen gestohlene Daten
Quelle des Falles	RTP-NOTICIAS[21]
Zeitraum des Auftretens	Aufgetreten zwischen Mai und Dezember 2017
Tags	Unternehmen, öffentliche Einrichtungen, Privatpersonen.
Status	Der Status dieses Falles ist abgeschlossen.
Anwendbarkeit Escape Room	Der Fall könnte auf das Escape-Room-Modell übertragen werden: Es handelt sich um einen wichtigen Fall, der untersucht werden sollte, vor allem angesichts der weitreichenden Auswirkungen und der Bekanntheit der Opfer (die zu schwerwiegenden Konsequenzen und zur Weitergabe vertraulicher Informationen hätte führen können). Wir haben Informationen über die technischen Aspekte des Angriffs (die Passwörter wurden durch Registrierungen auf Social-Media-Kanälen gestohlen, und die Daten wurden auf zwei Online-Listen - "Exploit.in" und "Anti Public" - veröffentlicht, die im Dark Web kursieren. Die Fall-Geschichte könnte in verschiedene Momente unterteilt werden: vom ersten Warnzeichen und der ersten Weitergabe von Daten (etwa 2016) bis zum Auffinden der endgültigen Listen und dem Bekanntwerden des Angriffs.

Was für ein Angriff war das?

Die Hacker nutzten Software-Schwachstellen in Servern öffentlicher Einrichtungen aus, die unter dem Gesichtspunkt der Cybersicherheit nicht ausreichend gewartet wurden.

Schwäche/Verwundbarkeit:

In dieser Situation können mehrere wichtige Fehler festgestellt werden:

- Berufliche und offizielle E-Mail-Adressen wurden von Einzelpersonen für die Registrierung auf sozialen Medienkanälen und anderen Plattformen verwendet.
- nach dem Vorfall keine Maßnahmen zum Schutz der aufgedeckten Konten getroffen wurden (z. B. durch Änderung der aufgedeckten Passwörter).

Was ist passiert?

- Der Quelle zufolge kursierte im Internet ein Dokument mit 20.416 Seiten (mit insgesamt fast 32,5 Millionen Passwörtern), das Daten von Mitarbeitern und Vertretern aus fast allen Bereichen der öffentlichen Verwaltung wie Ministerien, Streitkräften, öffentlichen Sicherheitskräften, Steuerbehörden und der nationalen Wahlkommission enthielt.

21 https://www.rtp.pt/noticias/pais/pj-confirma-ataque-informatico-milhares-de-passwords-roubadas_n1047761

- Die Opfer waren vielfältig und unterschiedlich: öffentliche Einrichtungen, große Unternehmen, Regierungsstellen, Angestellte des öffentlichen Dienstes und Fußballmannschaften.
- Darüber hinaus wurden auch Passwörter und E-Mails von Personen, die in privaten und öffentlichen Einrichtungen wie Banken, Krankenhäusern und Medien arbeiten, veröffentlicht. Nach den damals bekannt gewordenen Informationen wurden die persönlichen Daten der Nutzer bereits Jahre vor der Veröffentlichung gestohlen, und die Hacker hatten sie durch Angriffe auf Social-Media-Konten wie Facebook, LinkedIn und Twitter sowie auf Speicherplattformen wie Dropbox gesammelt. Dieser Angriff wurde als der größte jemals in Portugal registrierte Cyberangriff und der größte jemals verzeichnete Datendiebstahl bezeichnet.

Wie wurde sie wahrgenommen?

Am 20. Dezember 2017 veröffentlichte ein portugiesisches Nachrichtenmagazin einen Artikel, der enthüllte, dass Tausende von E-Mails und Passwörtern von einer Gruppe von Hackern gestohlen worden waren.

Welche Maßnahmen wurden ergriffen?

- Die Kriminalpolizei leitete umgehend Ermittlungen zu dem Anschlag ein. Ein Vertreter der Sicherheitskräfte räumte jedoch ein, dass die Informationen nicht neu und in der Tat schon länger (seit 2016) bekannt gewesen seien.
- Nach dem Vorfall wurden keine Maßnahmen ergriffen, um die aufgedeckten Konten zu schützen (z. B. durch Änderung der aufgedeckten Passwörter).

Was ist das Ergebnis der Schutzmaßnahmen?

In Anbetracht der Tatsache, dass viele der aufgedeckten Passwörter rund ein Jahr nach der Datenschutzverletzung[22] immer noch aktiv waren, kann der Schluss gezogen werden, dass es in mehreren öffentlichen und privaten portugiesischen Einrichtungen immer noch an Wissen über Online-Sicherheit mangelt.

22 https://tictank.pt/2017/12/22/contexto-sobre-a-maior-fuga-de-informacao-pessoal-em-portugal/

Fall 4 – Denial of Service in einem KMU

Titel	Denial of Service in einem KMU
Quelle des Falles	Interne Quelle
Zeitraum des Auftretens	Aufgetreten zwischen Januar und Februar 2022
Tags	KMU
Status	Der Status dieses Falles ist abgeschlossen.
Anwendbarkeit Escape Room	Der Fall könnte auf das Escape-Room-Modell übertragen werden, da er ein einfaches Problem zeigt, das die meisten KMU betreffen kann. Die technischen Aspekte des Falles sind leicht zugänglich.

Was für ein Angriff war das?

Denial of Service in einem KMU

Schwäche/Verwundbarkeit:

Die Ursache war ein Passwortangriff, der es ermöglichte, ein E-Mail-Konto eines Mitarbeiters zu kapern, das kein angemessenes Passwortgenerierungsschema verwendete.

Was ist passiert?

- Ein Passwort-Angriff, bei dem ein Konto gekapert wird. Die Hacker nutzten dann dieses Konto, um gefälschte E-Mail-Nachrichten zu generieren.
- Einige E-Mail-Konten und der E-Mail-Server wurden für Spam und Denial-of-Service-Attacken verwendet. Die KMU-Domäne wurde außerdem bei einigen Diensten auf die schwarze Liste gesetzt.

Wie wurde sie wahrgenommen?

Der Systemadministrator erhielt Hunderte von Warnungen über nicht oder an falsche Adressen gesendete Nachrichten. Dann meldete sich der Internetdienstanbieter und warnte vor der Situation.

Welche Maßnahmen wurden ergriffen?

Der Internet-Provider, der das KMU unterstützt, sperrte alle Zugänge zu den Websites und Online-Umgebungen mit Ausnahme derjenigen, die für die Verwaltung verwendet werden. Die Passwörter wurden geändert und die Dateien bereinigt. Es wurden bessere Kennwortdefinitionsverfahren eingeführt.

Was ist das Ergebnis der Schutzmaßnahmen?

Der Einbruch hat sich nicht wiederholt, obwohl es immer noch häufig zu Überfällen kommt.

Fall 5 – Code-Injektion auf Websites

Titel	Code-Einspeisung in Websites
Quelle des Falles	Interne Quelle
Zeitraum des Auftretens	Aufgetreten zwischen Oktober 2021 und März 2022
Tags	KMU
Status	Der Status dieses Falles ist abgeschlossen.
Anwendbarkeit Escape Room	Der Fall könnte auf das Escape-Room-Modell übertragen werden, da er ein einfaches Problem zeigt, das die meisten KMU betreffen kann. Die technischen Aspekte des Falles sind leicht zugänglich.

Was für ein Angriff war das?
Software-Exploit bei einigen WordPress-Plugins. Der Code wurde in diese Dateien injiziert.

Schwäche/Verwundbarkeit:
Die Mitarbeiter der KMU trafen keine geeigneten Maßnahmen zum Schutz der Formulare auf den Websites.

Was ist passiert?
Die Hacker nutzten ungeschützte Formulare auf den gehosteten Websites, um:
- auf einigen Seiten Codes zur Installation von Trojanern einzuschleusen.
- die Software auszuführen.
- Logbucheinträge zu generieren und Speicherplatz zu füllen.

Wie wurde sie wahrgenommen?
Der Internetdienstanbieter führt regelmäßige Sicherheitsprüfungen auf den Servern durch, auf denen der eingeschleuste Code entdeckt wurde.

Welche Maßnahmen wurden ergriffen?
Die Dateien wurden gesäubert und alle Plugins wurden aktualisiert.

Was ist das Ergebnis der Schutzmaßnahmen?
Der Einbruch hat sich nicht wiederholt, obwohl es immer noch häufig zu Überfällen kommt.

6. Schlussfolgerung

Die meisten der in diesem Kompendium dargestellten Fälle bestätigen, dass das Schutzniveau in KMU nicht mit der ständig wachsenden digitalisierten Innovation und dem Fortschritt in Einklang steht. Schwachstellen und Anfälligkeiten bestehen bei den Mitarbeitenden, die Endgeräte oft ohne die nötige Sorgfalt und Aufmerksamkeit für Cybersicherheit nutzen. Es mangelt nach wie vor an Kompetenzen und Wissen über Cyber-Bedrohungen sowie über das Ausmaß möglicher Schäden für das Unternehmen oder die eigene Person.

Die in drei europäischen Ländern gesammelten Beispiele haben gezeigt, dass die Probleme und Herausforderungen, mit denen europäische KMU konfrontiert sind, vergleichbar sind. Diese Ähnlichkeit ermöglicht die Erarbeitung gemeinsamer Lösungen zur Verbesserung des bestehenden Zustands. Generell ist es wichtig, auf die Risiken und individuellen Auswirkungen von unverändertem, unvorsichtigem und unbedachtem Verhalten hinzuweisen und eine Anleitung zum richtigen Handeln und Reagieren zu geben. Da kleine und mittlere Unternehmen zur wirtschaftlichen Stabilität in allen europäischen Ländern beitragen, ist es besonders wichtig, die Mitarbeitenden zu sensibilisieren und damit einen Beitrag zur Widerstandsfähigkeit und digitalen Sicherheit Europas zu leisten.

Art und Typ der Schwachstellen sind in allen KMU ähnlich und vergleichbar - sie umfassen Phishing, Social Engineering, Ransomware und unsichere Passwörter. Ein erheblicher Teil dieser Angriffe lässt sich auf menschliche Fehler zurückführen. Viele Unternehmen wendeten ähnliche Ansätze an, um den Angriffen zu begegnen und die Situation durch die Umsetzung technischer und organisatorischer Sicherheitsmaßnahmen zu bereinigen.

Dennoch haben nicht alle KMU-Führungskräfte die daraus gezogenen Lehren konsequent verinnerlicht. In mehreren Unternehmen richteten die Führungskräfte Präventivsysteme gegen Cyberangriffe und -bedrohungen ein, und nur wenige entschieden sich für Schulungen der Mitarbeitenden als weitere Sicherheitsmaßnahme. Diese Option scheint bisher weniger Priorität zu haben und weniger häufig verfolgt zu werden.

Die Reaktionen und Antworten auf Cyberangriffe in den vorgestellten KMU zeigen, dass das Verständnis und die Anerkennung der Bedeutung und des Wertes von Bildung und Ausbildung in diesem Bereich unzureichend sind. Diese Ergebnisse unterstreichen einmal mehr die dringende Notwendigkeit, Bildungsmöglichkeiten und -programme zu schaffen und anzubieten, die darauf abzielen, Kompetenzlücken beim nichttechnischen Personal zu verringern. Die Ausstattung von Unternehmen und Organisationen mit grundlegenden Kenntnissen und Fähigkeiten ist entscheidend für die Gewährleistung eines effektiven und sicheren Betriebs von Geschäftsprozessen.

Dieses Kompendium wurde veröffentlicht, um KMUs im Umgang mit relevanten Cybersicherheitsattacken zu unterstützen. Das EyesOnCS-Projekt selbst möchte einen Beitrag zur Cybersicherheitsschulung von Mitarbeitenden in europäischen KMUs und von Schülerinnen und Schülern von Berufsschulen leisten.

7. Referenzen

- Abt, C., Serious Games (1987): University Press of America.
- Agrawal, S.; Simon, A.; Bech, S.; Bæntsen, K.; Forchhammer, S. (2020): Defining immersion. Literature review and implications for research on audiovisual experiences. J. Audio Eng. Soc., 68, 404-417.
- ACN Italien: Nationale Cybersicherheitsstrategie 2022 - 2026, https://www.acn.gov.it/ACN_EN_Strategia.pdf, gesehen am 29.7.22.
- Bundesamt für Sicherheit in der Informationstechnik: Computer Emergency Response Team für Bundesbehörden (CERT-Bund), https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html, gesehen am 28.7.22.
- Informationen zur Cybersicherheit: National Cyber Security Centre Portugal (CNCS), https://www.cybersecurityintelligence.com/national-cyber-security-centre-portugal-cncs-2730.html, gesehen am 29.7.22.
- ENISA (2022): Konsolidierter jährlicher Tätigkeitsbericht 2021, Attiki, 2022.
- ENISA (2021): Cybersecurity for SMES- Challenges and Recommendations, Agentur der Europäischen Union für Cybersicherheit (ENISA), Attiki, 2021.
- Europäische Kommission: Der EU-Zertifizierungsrahmen für Cybersicherheit, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework, gesehen am 29.7.22.
- EUR-Lex: Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und die Zertifizierung für Cybersicherheit in der Informations- und Kommunikationstechnologie sowie zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Cybersicherheitsgesetz), 32019R0881 - DE - EUR-Lex, gesehen am 28.7.22.
- EyesOnCS Projektteam (2023): Cyber Alert Scenario_0x_nn, Vorbericht des Projektteams, wird noch veröffentlicht, FHM Düren, Düren, 2023
- Guckian,. J., Sridhar, A. & Meggitt, S. J. (2020): Erforschung der Perspektiven von Dermatologie-Studenten mit einem Escape-Room-Spiel. Klinische und experimentelle Dermatologie, 45 (2), 153-158. https://doi.org/10.1111/ced.14039

- Juzeleniene, S., Mikelioniene, J., Escudeiro, P., Vaz de Carvalho, C. (2014): GABALL project. serious games-based language learning. Procedia-Soc. Behav. Sci. 136, 350-354.

- Mac Gregor, M. (2018). Campus Clue: Habituating Students to the Information Search Process via Gaming. Pennsylvania Libraries: Research & Practice, 6 (2), 86-92. https://doi.org/10.5195/palrap.2018.172

- Martina, Richard & Göksen, Sultan. (2020). Developing Educational Escape Rooms for Experiential Entrepreneurship Education. Entrepreneurship Education and Pedagogy. https://www.researchgate.net/publication/346548119_Developing_Educational_Escape_Rooms_for_Experiential_Entrepreneurship_Education , gesehen am 10.1.23.

- Michael, D.R., Chen, S.L. (2006): Serious Games. Games That Educate, Train, and Inform. Thomson Course Technology PTR, Oshawa.

- N.N.: https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks/ , gesehen 28.7.22.

- N.N.: Über ENISA - Die Agentur der Europäischen Union für Cybersicherheit, https://www.enisa.europa.eu/about-enisa/about-enisa-the-european-union-agency-for-cybersecurity, gesehen 28.7.22.

- N.N.: https://www.django-hurtig.com/jagdzentrum/jagd_vorgang_mainstream_id.php?id2=21727, gesehen 28.7.22.

- N.N.: https://www.dn.pt/sociedade/servicos-de-voz-movel-da-vodafone-registam-recuperacao-progressiva-14568590.html, gesehen 28.7.22.

- N.N.: https://www.dn.pt/dinheiro/fraude-marca-continente-alvo-de-phishing-11487091.html, gesehen 28.7.22.

- N.N.: https://www.rtp.pt/noticias/pais/pj-confirma-ataque-informatico-milhares-de-passwords-roubadas_n1047761, gesehen 28.7.22.

- N.N.: https://tictank.pt/2017/12/22/contexto-sobre-a-maior-fuga-de-informacao-pessoal-em-portugal/, gesehen 28.7.22.

- N.N.: https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks/, gesehen 28.7.22.

- N.N.: Deutschland sicher im Netz, https://www.sicher-im-netz.de, gesehen 28.7.22.

- Oblinger, D. (2006): Simulationen, Spiele und Lernen. ELI White Paper, Bd. 1, Nr. 1. http://net.educause.edu/ir/library/pdf/ELI3004.pdf.

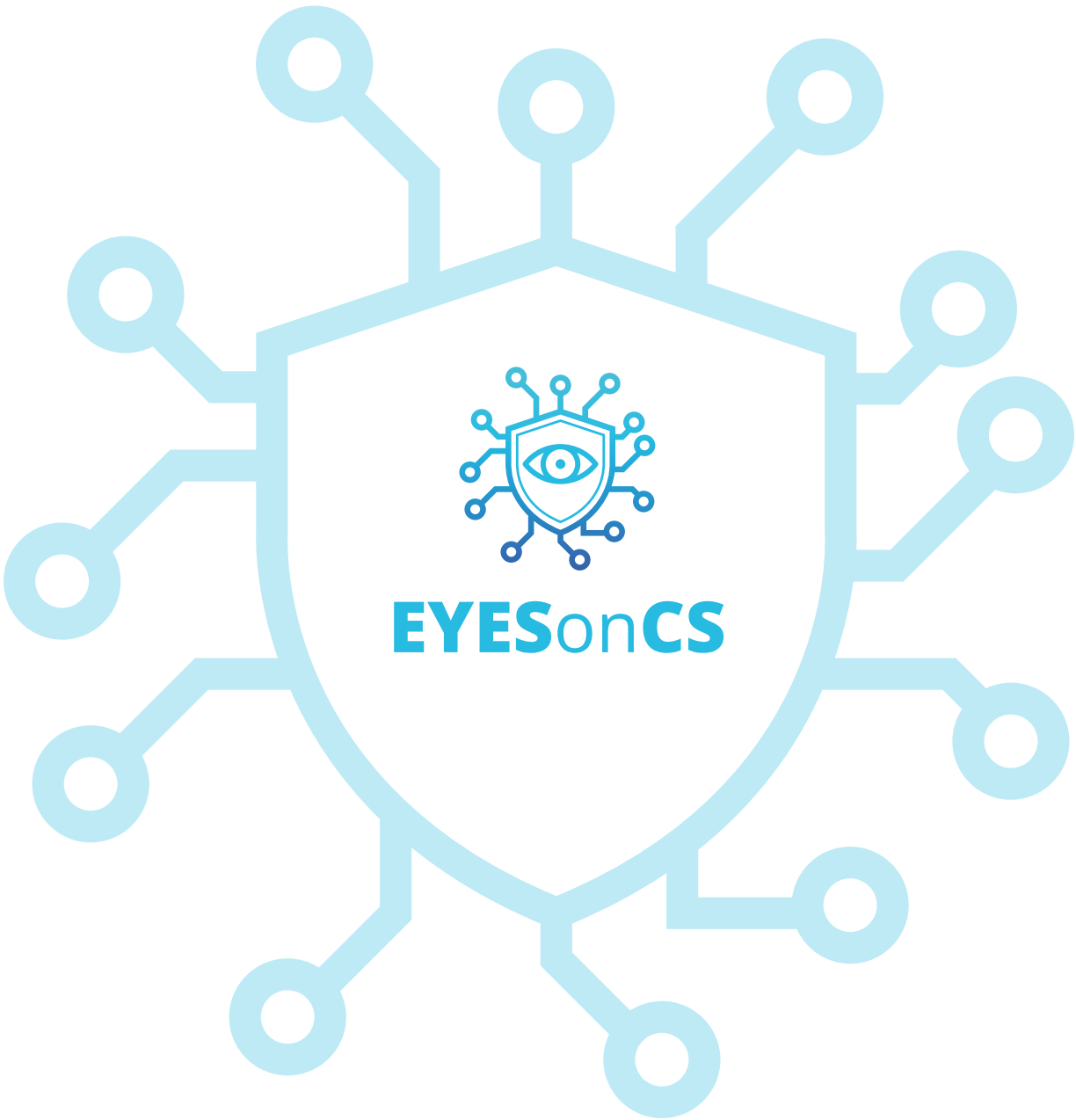
- Prensky, M. (2003): Digital Game-Based Learning. Comput. Entertain. (CIE) 1(1), 21.

- Streim, A., Mann, S. (2021): Angriffsziel deutsche Wirtschaft: mehr als 220 Milliarden Euro Schaden pro Jahr, bitkom, https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr, gesehen am 2.3.23

- Tercanli, H., Martina, R., Ferreira Dias, M., Reuter, J., Amorim, M., Madaleno, M., Magueta, D., Vieira, E., Veloso C., Figueiredo, C., Vitòria, A., Wakkee, I., Gomes, I., Meireles, G., Daubariene, A., Daunoriene, A., Mortensen, A., Zinovyeva, A., Rivera-Trigueros, I., Lòpez-Alcarria, A., Rodrigìguez-Dìaz, P., Olvera-Lobo, M.D., Ruiz-Padillo, D.P., And Guitièrrez-Pèrez, J. (2021), Educational escape rooms in practice: Forschung, Erfahrungen und Empfehlungen. UA Editoria. https://doi. org/10.34624/rpxk-hc61

- Zyda, M. (2005): Von der visuellen Simulation über die virtuelle Realität zum Spiel. Computer 38(9), 25-32.

Notizen



Bleiben Sie dran!
Folgen Sie uns und erfahren
Sie mehr über das Projekt unter:

www.eyesoncs.eu

Kofinanziert von der
Europäischen Union