Leistungsbeschreibung

Cybersecurity Assessments

Die Cybersecurity Assessments der audatis Cert GmbH dienen der Beurteilung des Sicherheitsniveaus von Schnittstellen und Systemkomponenten eines Unternehmensnetzwerks sowie der Mitarbeiterawareness gegenüber Cyberangriffen. Darüber hinaus können sie als Nachweis der Wirksamkeit der technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO dienen. Auf Grundlage der Beurteilung werden Maßnahmen abgeleitet, welche die Widerstandsfähigkeit eines Unternehmens gegen Cyberangriffe erhöhen. Die Begutachtung erfolgt durch eine gezielte Suche, Bewertung und ggf. Ausnutzung von Schwachstellen innerhalb der Systemkomponenten. Neben der Expertise des Prüfers und selbstentwickelten Richtlinien basiert das Vorgehen, soweit möglich, auf öffentlich zugänglichen Standards, die von Organisationen wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI), dem Open Web Application Security Project (OWASP), der Open Source Security Testing Methodology Manual (OSSTMM) und dem National Institute of Standards and Technology (NIST) veröffentlicht wurden.

Die in Herford ansässige audatis Cert GmbH ist auf die Durchführung von Audits, Überprüfungen und Zertifizierung im Bereich der Informationssicherheit und des Datenschutzes spezialisiert und sichert die Unabhängigkeit aller Überprüfungshandlungen sowie der daran beteiligten Prüfer zu.

Inhaltsverzeichnis

1. Ablauf eines Cybersecurity Assessments

Im Rahmen eines Cybersecurity Assessments wird ein realer Cyberangriff simuliert, um so die Schwachstellen und potenziellen Einfallstore in ein Unternehmen aufzudecken und diese im Nachgang mit entsprechenden Maßnahmen schließen zu können. Ein Cyberangriff erfolgt typischerweise nicht linear und basiert auf der Ausnutzung von Schwachstellen unterschiedlicher Ebenen. Dennoch lassen sich grundsätzlich drei Phasen unterscheiden, diese werden nachfolgend kurz beschrieben.

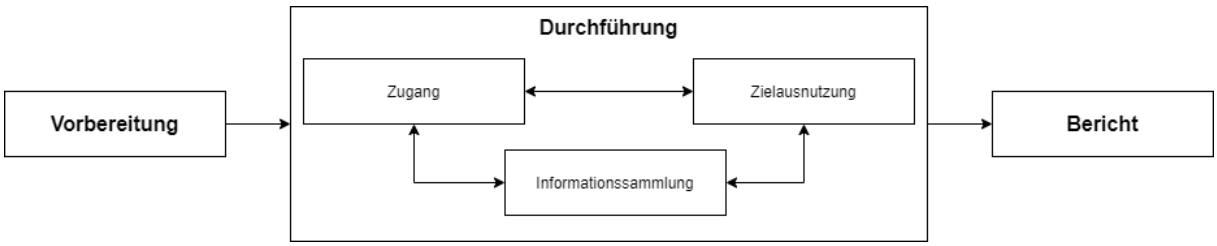

Abbildung 1:Cybersecurity Assessment

1.1 Vorbereitung

Während der Vorbereitung werden alle relevanten Rahmenparameter mit dem Auftraggeber abgestimmt. Dazu zählt unter anderem:

- Umfang des Assessments (s. Abschnitt 2)
- Durchführungszeiten, Besprechungstermine und Projektmeilensteine
- Vorbereitung und Prüfung aller benötigten Zugänge

Zudem passt der Prüfer die nötigen Werkzeuge und die Infrastruktur entsprechend des Bewertungsziels an.

1.2 Durchführung

Die Durchführungsphase beinhaltet die Kernaktivitäten Zugang, Informationssammlung und Zielausnutzung. Die Teilergebnisse dieser drei Tätigkeiten beeinflussen oder ermöglichen weitere Ansatzpunkte in dem fortschreitenden Cybersecurity Assessment. Dementsprechend werden alle Kernaktivitäten mehrfach durchlaufen.

1.2.1 Informationssammlung

Informationen über das Bewertungsziel, wie z.B. IP-Adressen, Domainnamen, Mitarbeiternamen, Geschäftspartnernamen oder unternehmensinterne Informationen, bilden die Grundlage eines jeden Angriffs und werden daher durchgängig während eines Cybersecurity Assessments gesammelt, strukturiert und analysiert. Die Strukturierung der Informationen erfolgt u.a. durch eine Erstellung von Architekturdiagrammen, die virtuelle, soziale und physische Betrachtungsebenen abbilden. Mögliche Informationsquellen sind:

- Von dem Auftraggeber zur Verfügung gestellte Informationen (s. Vorbereitung)
- Durch Zugangs- oder Zielausnutzungsaktivitäten gesammelte Informationen
- Im Rahmen der Analyse selbst ermittelte Informationen

Darüber hinaus erfolgt mithilfe von spezialisierten Werkzeugen eine gezielte Suche nach sensiblen Informationen über das Unternehmen, deren öffentliche Verfügbarkeit den Verantwortlichen nicht bekannt ist oder deren Kritikalität unterschätzt wird.

1.2.2 Zielausnutzung

Das finale Ziel eines Cybersecurity Angriffs ist typischerweise die Kompromittierung eines Netzwerks, Hosts oder einer Applikation. Eine Kompromittierungen kann die Übernahme der Kontrolle oder die unerlaubte Entnahme von Informationen (Kundendaten, Geschäftsgeheimnisse etc.) von Netzwerken, Hosts oder Applikationen bedeuten, dies erfolgt typischerweise durch die Ausnutzung von Schwachstellen. Hosts sind alle Geräte (Desktop PC, Server, Smartphone etc.), welche an ein Netzwerk angeschlossen sind, Betriebssysteme werden im Rahmen von Hosts untersucht. Applikationen sind ausführbare Software Programme (Microsoft Teams, unternehmenseigene Webapplikationen etc.), Dienste werden im Rahmen von Applikationen untersucht. Neben der Suche nach sensiblen Informationen ist die strukturierte Suche nach ausnutzbaren Schwachstellen somit das Hauptziel dieser Kernaktivität. Das konkrete Vorgehen hängt stark von den verwendeten Technologien des Bewertungsziels ab.

1.2.3 Zugang

Die Kernaktivität Zugang beschäftigt sich mit der Öffnung von Zugängen zum Bewertungsziel. Sie kommt typischerweise zum Einsatz, wenn bereits bekannte Systemkomponenten nicht oder nur schwer ausgenutzt werden können (s. 1.2.2). Zugänge können zu Netzwerken, Hosts oder Applikationen geschaffen werden.

Zugangsaktivitäten werden in Form von Szenarien durchgeführt, die primär auf Social Engineering und physischen Angriffsmethoden basieren. Nachfolgend werden zwei Beispielszenarien grob beschrieben (eine detaillierte Beschreibung der Zugangsszenarien befindet sich im Anhang):

Bulk Phishing Szenario

Der Prüfer sendet eine generalisierte E-Mail an alle Mitarbeiter des Unternehmens und fordert diese auf, einem Link zu folgen. Der Link führt zu einer gefälschten Login Seite von Microsoft (Phishing). Falls ein Mitarbeiter seine Zugangsdaten eingibt, ist ein Zugang zu einer Applikation eröffnet.

USB Dropping Szenario

Der Prüfer besucht das Unternehmen vor Ort und platziert modifizierte USB-Sticks an zuvor abgestimmten Orten, z.B. Parkplatz oder am Empfang. Falls ein Mitarbeiter den USB-Stick in einem Computer des Unternehmens einsteckt, ist damit ein Zugang zu einem Host eröffnet.

Nach einer erfolgreichen Zugangsaktivität kann der Prüfer mit einer Zielausnutzung fortfahren.

1.3 Bericht

In der Phase der Berichtserstellung dokumentiert der Prüfer alle von ihm vorgenommenen Tätigkeiten und Erkenntnisse. Den Testergebnissen wird eine Kritikalität zugeordnet, die aussagt, welcher Schaden bei erfolgreicher Ausnutzung entstehen kann. Weiterhin enthält der Bericht Handlungsempfehlungen zur Behebung der Schwachstellen und eine zusammenfassende Sicherheitsbeurteilung des Prüfers. Auf Basis des Berichts wird zudem ein Abschlussgespräch mit dem Auftraggeber durchgeführt, um mögliche Fragestellung zu klären.

2. Umfang eines Cybersecurity Assessments

Das Vorgehen der audatis Cert GmbH basiert auf einem authentischen und ganzheitlichen Ansatz, der auch als Red Team Assessment bezeichnet wird. Dies ermöglicht die praxisnahe Einschätzung der Angreifbarkeit eines Unternehmens. Aufgrund der Komplexität realer Cyberangriffe erfordert ein Red Team Assessment eine umfangreiche Prüfung des Bewertungsziels. Dieser Umfang kann in Abhängigkeit von Ressourcenverfügbarkeit und Sicherheitsbedürfnis des Auftraggebers reduziert werden. Die folgenden Parameter können dabei angepasst werden:

2.1 Informationssammlung

Die vertiefte Suche von Informationen in öffentlichen Quellen (OSINT) über das Bewertungsziel, wie z.B. IP-Adressen, Mitarbeiternamen, Geschäftspartnernamen oder unternehmensinterne Informationen, kann ausgeschlossen werden. Dies hat zur Folge, dass keine Aussage über die öffentliche Verfügbarkeit sensibler Informationen und deren Relevanz für einen realen Angriff getroffen werden kann.

2.2 Netzwerk, Host und Applikation

Das Cybersecurity Assessment kann auf bestimmte Netzwerke, Hosts und Applikationen beschränkt werden, z.B. auf einen Webshop. Falls eine Beschränkung auf dieser Ebene vorliegt, spricht man typischerweise von einer Schwachstellenanalyse oder einem Penetrationstest auf die freigegebenen Systemkomponenten. Diese isolierte Betrachtung von Hosts hat zur Folge, dass mögliche Angriffsvektoren über nicht betrachtete Komponenten unentdeckt bleiben.

2.3 Untersuchungstiefe

Die Untersuchung von Hosts und Applikationen während der Zielausnutzungs-Phase beginnt immer mit der Suche nach ausnutzbaren Schwachstellen. Dazu werden zunächst primär automatisierte Werkzeuge eingesetzt und die daraus resultierenden Ergebnisse anschließend manuell verifiziert und bewertet. Dies wird auch als Schwachstellenanalyse bezeichnet und bildet die Basis jeder Untersuchung. Im Anschluss an die Schwachstellenanalyse beginnt der Prüfer mit einer tiefgehenden manuellen Analyse des Bewertungsziels. Diese ermöglicht die Identifikation weiterer Schwachstellen, sowie eine Einschätzung der Widerstandsfähigkeit des Bewertungsziels gegenüber gezielten Cyberangriffen. Darüber hinaus nutzt der Prüfer die identifizierten Schwachstellen aktiv aus, kombiniert Angriffsmethoden miteinander und bewertet das Schadenspotenzial nach Ausnutzung der Schwachstellen. Dieses Vorgehen wird als Penetrationstest bezeichnet.

Ein Cybersecurity Assessment kann auf die Durchführung von Schwachstellenanalysen eingeschränkt werden. In diesem Zuge wird das Assessment auf die Simulation eines primär automatisierten Massenangriffs reduziert und das Bewertungsziel nur auf ein Mindestmaß an Widerstandsfähigkeit gegenüber Cyberangriffen geprüft.

2.4 Ausgangsperspektive

Die Ausgangsperspektive bestimmt den Detailgrad der Systeminformationen, die dem Prüfer während der Durchführung des Assessments zur Verfügung stehen. Grundsätzlich können zwei Ansätze unterschieden werden:

- **Blackbox**: Der Prüfer erhält nur Informationen, um das Bewertungsziel zu erreichen, z.B. eine IP Adresse.
- **Greybox** / **Whitebox**: Der Prüfer erhält bestimmte oder alle bekannten Systeminformationen, z.B. Administratorzugänge oder Netzwerkarchitekturen.

Die im Rahmen einer Greybox Perspektive verfügbaren Informationen können einem echten Angreifer aus verschiedenen Gründen zur Verfügung stehen, z.B.:

- Böswillige Mitarbeiter
- Unachtsame Mitarbeiter (OSINT oder Social Engineering)
- Bereits kompromittierte Systemkomponenten

Ein direkter Vergleich der Ausgangsperspektiven zeigt, dass die Greybox Perspektive typischerweise deutlich mehr Schwachstellen aufgedeckt. Gleichzeitig ist diese Ausgangsperspektive mit mehr Aufwand verbunden, da mehr Systemkomponenten und Informationen untersucht werden müssen.

In der Praxis ist häufig eine Mischform die beste Wahl, in der das Assessment zunächst aus einer Blackbox Perspektive gestartet wird und zu einem bestimmten Zeitpunkt weitere Informationen oder Zugänge vom Auftraggeber freigegeben werden, da Blackbox-Angriffe zwar deutlich häufiger stattfinden, Greybox-Angriffe jedoch meist erfolgreicher sind. Das konkrete Vorgehen wird zwischen dem Auftraggeber und dem Prüfer während der Vorbereitung abgestimmt.

2.5 Zugangsszenarien

Die Durchführung von bestimmten Zugangsszenarien (s. Anhang) kann vollständig oder teilweise ausgeschlossen werden. Da Zugangsszenarien, insbesondere Phishing Angriffe, den primären Einstiegsweg in Unternehmensnetzwerke darstellen, mindert diese Reduktion die Aussagekraft des Cybersecurity Assessments erheblich.

Alternativ kann das Cybersecurity Assessment auch auf die Durchführung einzelner Zugangsszenarien beschränkt werden. Diese werden dann isoliert durchgeführt, um Schwachstellen auf sozialer oder physischer Ebene zu identifizieren. So kann z.B. eine generalisierte Phishing Kampagne durchgeführt werden, um das Sicherheitsbewusstsein aller Mitarbeiter in Bezug auf diesen Angriffsvektor zu prüfen.

2.6 Externe Systemkomponenten

Falls der Auftraggeber Systemkomponenten verwendet, welche sich nicht in seinem Eigentum befinden, muss die Freigabe auf diese Komponenten im Rahmen der Vorbereitung von dem Eigentümer eingeholt werden. Falls dies nicht möglich ist, müssen diese Komponenten von dem Cybersecurity Assessment ausgeschlossen werden.

3. Testate und Siegel

Wird bei einem Cybersecurity Assessment keine kritische Schwachstelle identifiziert, verleiht die audatis Cert GmbH ein Testat sowie ein Gütesiegel, welches z.B. auf der Website des Auftraggebers veröffentlicht werden darf. Eine Schwachstelle wird als kritisch klassifiziert, wenn durch ihre Ausnutzung vertrauliche Unternehmensdaten entnommen werden konnten.

Die Vergabe eines Testats ist abhängig von den zuvor vereinbarten Einschränkungen. Falls das Cybersecurity Assessment ohne Einschränkungen auf Unternehmensebene durchgeführt wurde (Red Team Assessment), wird das Testat für das gesamte Unternehmen ausgestellt. Wurde das Cybersecurity Assessment auf eine manuelle Hostanalyse mit Greybox Ausgangsperspektive eingeschränkt (Penetrationstest), erhalten die untersuchten Systemkomponenten ein Testat (z.B. Webshop). Für automatisierte Schwachstellenanalysen und isoliert durchgeführte Zugangsszenarien werden keine Testate und Gütesiegel verliehen. Bei Bedarf kann neben dem internen Bericht jedoch ein Bericht zur Veröffentlichung erstellt werden.

Die Gültigkeitsdauer der Testate beträgt ein Jahr und kann im Rahmen einer Teilprüfung verlängert werden. Die Behebung von kritischen Schwachstellen kann ebenfalls durch eine Teilprüfung nachgewiesen werden und führt zum Erlangen des Testates.

Alle Cybersecurity Assessments können als Nachweis der Wirksamkeit der technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO verwendet werden.

4. Kosten

Im Rahmen eines kostenfreien Erstgesprächs wird zunächst in Abhängigkeit von den verfügbaren Ressourcen und dem Sicherheitsbedürfnis des Auftraggebers der gewünschte Umfang ermittelt. Auf dieser Basis wird der individuelle Projektaufwand anhand der Rahmenparameter Branche, Schutzbedarf der verarbeiteten Informationen, Sicherheitsziele des Auftraggebers und Unternehmensgröße kalkuliert.

Eine Kontaktaufnahme zur Terminabsprache ist jederzeit möglich.

5. Ansprechpartner

Marcel Albrink
Consultant Informationssicherheit

Schwerpunkte: Penetrationstests, Sichere Softwareentwicklung

Mail: m.albrink@audatis.de
Fon: 05221 87292-06

Sascha Knicker
Senior Consultant Datenschutz und Informationssicherheit

Schwerpunkte: Datenschutz, TISAX, ISO 27001

Mail: s.knicker@audatis.de
Fon: 05221 87292-07

Anhang: Beschreibung der Zugangsszenarien

Phishing Szenarien

Phishing Angriffe gehören weiterhin zu der häufigsten Methode von Cyber Angriffen. Laut einer Studie von Trend Micro wurden 39% der befragten deutschen Unternehmen bereits Opfer eines entsprechenden Angriffs. Diese Angriffe nehmen die „Schwachstelle Mensch“ ins Visier. Um sich wirksam zu schützen, sollten Unternehmen neben einer zeitgemäßen IT Sicherheitslösung vor allem in die Sensibilisierung ihrer Mitarbeiter investieren.

Alle Phishing Szenarien beinhalten ein E-Learning Programm für die Teilnehmer des Szenarios, das folgende Punkte enthält:

- Definition von Phishing
- Konsequenzen und Schaden von Phishing Angriffen in Deutschland
- Merkmale und Abwehrmöglichkeiten von Phishing E-Mails

Zudem erhalten die Teilnehmer eine grafische Zusammenfassung der wichtigsten Merkmale von Phishing E-Mails und ein 30-minütiges Webinar zur Beantwortung von Fragestellungen.

Bulk Phishing Szenario

Im Rahmen eines Bulk Phishing Szenarios wird eine generische (nicht auf den individuellen Mitarbeiter personalisierte) E-Mail erstellt und bietet damit die Möglichkeit eine möglichst große Anzahl Mitarbeiter zeitgleich zu prüfen.

Im Rahmen der Vorbereitung wird eine primäre Standardsoftware des Unternehmens, wie z.B. Microsoft Office 365 oder Google G Suite, als Ausgangspunkt gewählt. Hierauf aufbauend erstellt der Prüfer ein Phishing Angriffs Szenario (s. beispielhaft Abbildung: Ausschnitt Phishing E-Mail). Typischerweise wird der Empfänger in einer Phishing E-Mail dazu aufgefordert einem Link zu einer Phishing Website zu folgen. Auf dieser wird er anschließend aufgefordert, seine Zugangsdaten einzugeben. Im Anschluss an die Erstellung des Szenarios wird in Zusammenarbeit mit dem Auftraggeber die Zustellbarkeit und Plausibilität des Szenarios geprüft.

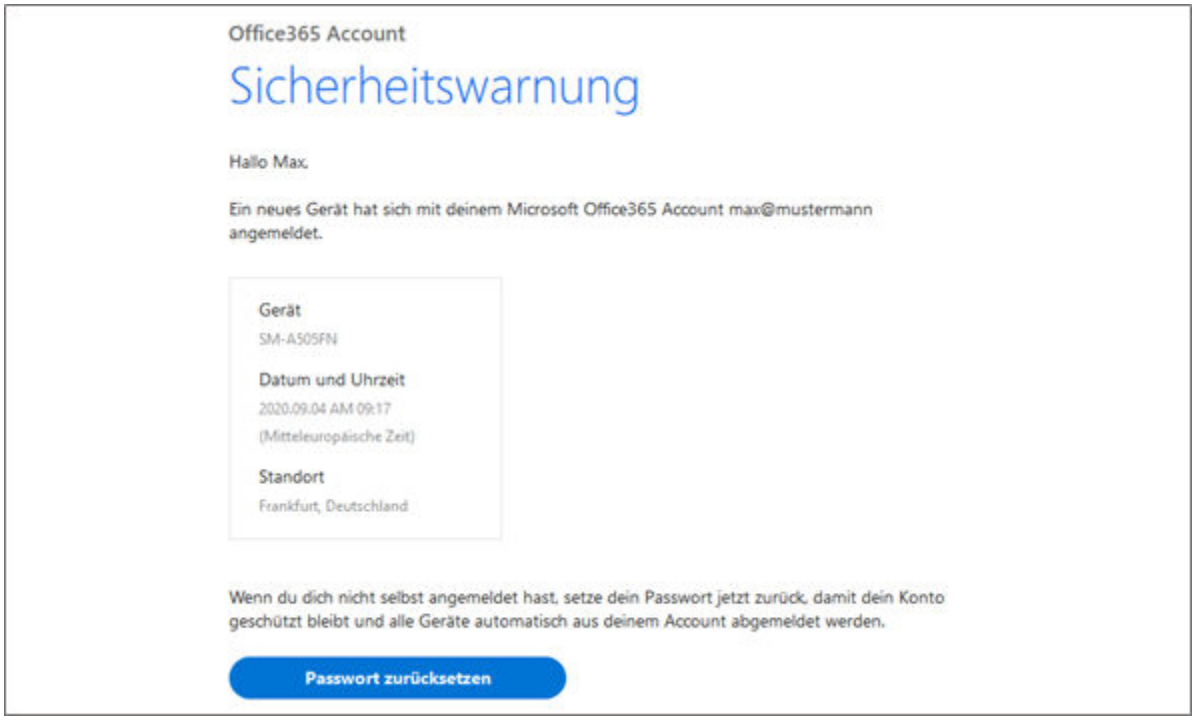

Abbildung 2: Ausschnitt Phishing E-Mail

In der Durchführungsphase wird die Phishing E-Mail an alle Teilnehmer des Szenarios gesendet und die Reaktion dieser aktiv untersucht. Der Prüfer hat dabei die Möglichkeit Mitarbeiter zu identifizieren, welche:

- die E-Mail geöffnet haben (kann durch bestimmte E-Mail Clients geblockt werden)
- den Link gefolgt sind (sichere Zuweisung)
- Benutzerdaten auf der gefälschten Website eingegeben haben (sichere Zuweisung)

Gibt ein Teilnehmer seine Zugangsdaten ein, wird er durch eine eindrucksvolle Warnmeldung auf den Sachverhalt und die möglichen Konsequenzen seines Verhaltens hingewiesen.

In der Auswertungsphase erstellt der Prüfer einen Bericht, welcher die Erkenntnisse der Untersuchungen zusammenfasst und das Sensibilisierungsniveau der Teilnehmer bewertet.

Zuletzt werden in einem kurzen Abschlussgespräch die Ergebnisse besprochen und evtl. weitere Maßnahmen vorgestellt.

Spear Phishing Szenario

Ein Spear Phishing Szenario zielt darauf ab, bestimmte Mitarbeiter mithilfe individualisierter Phishing E-Mails zu sensibilisieren. Dieses Vorgehen erschwert die Erkennung für den Teilnehmer erheblich, gleichzeitig beschränkt es die Anzahl der Mitarbeiter die gleichzeitig sensibilisiert werden können ebenfalls deutlich ein. Typischerweise werden im Rahmen eines Spear Phishing Szenarios daher nur Mitarbeiter sensibilisiert, welche Zugriff auf besonders sensible Daten haben, wie z.B. Abteilungsleiter oder Systemadministratoren.

Die Erstellung eines Spear Phishing Szenarios basiert häufig auf einer Vielzahl von Informationen und ist damit deutlich komplexer als die Erstellung eines Bulk Phishing Szenarios. Die Informationen können sowohl durch Informationssammlungs-Aktivitäten (s. Kapitel 1.2.1) beschafft werden oder durch den Auftraggeber bereitgestellt werden (s. Ausgangsperspektive in 1.1). Ersteres bildet einen authentischen externen Angriff nach, während zweiteres den Projektaufwand reduziert.

Die Durchführungs- und Auswertungsphase entspricht dem Vorgehen bei einem Bulk Phishing Szenario.

Hinweis zur Auswertung und Mitbestimmungsrechten bei Phishing Szenarien

Zur Durchführung simulierter Phishing Angriffe im Rahmen einer Sensibilisierungskampagne werden personenbezogene Daten der Mitarbeiter verarbeitet (mindestens Namen und E-Mail Adressen) und das entsprechende Verhalten zu Auswertungszwecken dokumentiert.

Dabei kann es sich um sog. verhaltensbasierte Daten handeln (klickt ein Mitarbeiter auf die Links oder gibt er sensible Daten preis), bei welchen die Mitbestimmungsrechte einer evtl. vorhandenen Mitarbeitervertretung (z.B. Betriebs- oder Personalrat) berücksichtigt werden müssen.

Dem Auftraggeber werden grundsätzlich aus Datenschutzgründen im Rahmen der Kampagnen keine Detailergebnisse einzelner Mitarbeiter weitergegeben, sondern lediglich anonyme Kennzahlen im Rahmen der Auswertung und Executive Summary. Damit sind solche Kampagnen auch als Sensibilisierungsmaßnahme gem. Art. 39 DS GVO durchführbar und halten die Anforderungen von Mitarbeitervertretern und Datenschutzgesetzen ein.

Auf Wunsch kann der Auftraggeber eine personenbezogene Auswertung erhalten, sofern die mitbestimmungsrechtlichen und datenschutzrechtlichen Voraussetzungen erfüllt sind und dies bei der Beauftragung zugesichert wurde.

USB Dropping Szenario

USB Dropping ist eine spezielle Form eines Baiting Angriffs (Social Engineering). Bei diesem Angriff werden manipulierte USB Sticks gezielt in der physischen Nähe des Ziels platziert, z.B. auf Parkplätzen oder in öffentlich zugänglichen Räumlichkeiten eines Unternehmens. Im Rahmen eines realen Angriffs sind die platzierten USB Sticks häufig mit Malware präpariert.

Die Gefahr von unbekannten USB Sticks wird von ungeschultem Personal häufig stark unterschätzt, so hat eine Studie[1] aus dem Jahr 2016 ergeben, dass mindestens 45% der Angriffe dieser Art erfolgreich sind. Hinzu kommt, dass es nur wenig technische Abwehrmechanismen gegen USB Dropping Angriffe gibt.

Im Rahmen eines USB Dropping Szenarios werden präparierte USB Sticks an einem Standort des Auftraggebers platziert. Diese USB Sticks enthalten keine schädliche Malware, sie enthalten jedoch standardmäßig ein Skript, welches dem Prüfer aufzeigt, ob der USB Stick in einen Computer mit Internet Anbindung gesteckt wurde. Weiterhin wird dem Benutzer des Computers eine eindrucksvolle Warnmeldung gezeigt, welche auf den Sachverhalt und die möglichen Konsequenzen seines Verhaltens hinweist. Das Verhalten der USB Sticks bei Aktivierung kann je nach Bedarf angepasst werden.

WiFi Attack Szenario

Schwachstellen in WiFi Netzwerken können einem Angreifer einen schnellen und einfachen Weg in das interne Unternehmensnetzwerk bieten. Eine Untersuchung des Kaspersky Security Network[2] hat ergeben, dass weltweit mehr als ein Viertel der WiFi Netzwerke unsichere oder keine WiFi Verschlüsselung nutzen. Neben dem Verschlüsselungsprotokoll gibt es eine Vielzahl weiterer Angriffsvektoren gegen kabellose Netzwerke.

Während eines WiFi Attack Szenarios wird ein WiFi Netzwerk vor Ort von einem Prüfer untersucht. Dabei wird das WiFi Netzwerk zunächst bewertet und anschließend entsprechend der verwendeten Technologien angegriffen.

In der Auswertungsphase erstellt der Prüfer einen Bericht, welche alle identifizierten Schwachstellen und mögliche Maßnahmen deren Behebung enthält.

Haftung und Versicherung bei Cybersecurity Assessments

Die Deckungssumme im Schadensfall richtet sich nach der jeweils aktuellen max. Deckung durch unseren Versicherungsgeber (Hiscox AG) mit derzeit 2,5 Mio. EUR für Sach- und Vermögenschäden, 3 Mio. EUR für Personenschäden. Auf Wunsch kann die Versicherungssumme gegen Aufpreis erhöht werden.

[1] Users Really Do Plug in USB Drives They Find, abrufbar unter: https://elie.net/static/files/users-really-do-plug-in-usb-drives-they-find/users-really-do-plug-in-usb-drives-they-find-paper.pdf

[2] Research on unsecured Wi Fi networks across the world, abrufbar unter: https://securelist.com/research-on-unsecured-wi-fi-networks-across-the-world/76733/