GCA Cybersicherheitstoolkit für KMU: Handbuch

Willkommen

Sehr geehrte Kollegen,

das Internet ist heutzutage ein fester Bestandteil des Geschäfts der meisten Unternehmen. Die Sicherung des digitalen Ökosystems Ihres Unternehmens muss Teil Ihrer Arbeitsweise sein. Ein Cyberangriff kann verheerende Folgen haben, einschließlich finanzieller Verluste, Diebstahl sensibler Informationen, beeinträchtigter Lieferketten und mehr.

Sie haben viele andere Sorgen und Verantwortlichkeiten, und wir haben daran gearbeitet, eine Ressource bereitzustellen, die Sie tatsächlich nutzen können, um Ihren Bedarf an Cybersicherheit zu decken. Das Global Cyber Alliance (GCA) Cybersicherheitstoolkit für KMU bietet kostenlose und effektive Tools zur Reduzierung Ihres Cyberrisikos. Die Tools sind sorgfältig ausgewählt und organisiert, um es einfach zu machen, wichtige Schritte zu finden und zu implementieren, die helfen, Ihr Unternehmen gegen Cyber-Bedrohungen zu schützen. Wir haben Videos sowie ein Community-Forum hinzugefügt, in dem Sie Unterstützung finden und Antworten auf Fragen von Ihren Kollegen und Sicherheitsexperten finden können. Das Toolkit ist für Sie konzipiert, kein hypothetisches kleines Unternehmen mit Cybersicherheitsexperten für Mitarbeiter und einem großen Budget.

Das Handbuch zum GCA Cybersicherheitstoolkit für KMU ist ein Begleiter des Toolkits, der Ihnen das Toolkit näher erläutert. Sie können das Handbuch vollständig oder Kapitel für Kapitel herunterladen, während Sie sich durch die empfohlenen Aktionen im Toolkit durcharbeiten. Dieser Leitfaden erleichtert Ihnen die Möglichkeit, in Ihrem eigenen Tempo zu arbeiten, um Maßnahmen zu ergreifen, und ist ein praktisches Referenzdokument.

Diese Ressourcen werden regelmäßig mit Beiträgen von Anwendern, Branchenexperten und Partnern auf der ganzen Welt aktualisiert.

Wir hoffen, dass Sie das Toolkit und das Handbuch nutzen, um Ihre Cybersicherheit noch heute zu verbessern!

Mit freundlichen Grüßen

Philip Reitinger
Präsident und CEO

Inhaltsverzeichnis

Handbuch-Kapitel

Kennen Sie Ihre eigene IT-Umgebung

Welches Problem spricht diese Toolbox an?

Zu wissen, was man hat, ist der erste Schritt zu mehr Sicherheit, denn man kann nichts schützen, wenn man sich deren Existenz nicht bewusst ist. Bedenken Sie, dass viele Cyberangriffe und Datenverstöße durch verlorene oder gestohlene Laptops und andere Geräte, unbefugten Zugriff auf Konten und nicht gepatchte Softwareschwachstellen verursacht werden. Wenn Sie wissen, über welche Computer, Geräte und Software Sie verfügen (d. h. Ihre Vermögenswerte), werden Sie potenzielle Risiken, die möglicherweise bestehen, besser verstehen, was Ihnen ermöglicht, fundierte Entscheidungen zu treffen und Schritte zur Verringerung dieser Risiken einzuleiten.

- Wissen Sie, wie viele Laptops und Mobilgeräte Ihr Unternehmen hat, wer Zugriff darauf hat und welche Software und Anwendungen auf ihnen installiert sind?
- Wissen Sie, wie alt Ihre Computer sind und wann Sie ihre Sicherheitsvorkehrungen zuletzt aktualisiert haben?
- Verfügen Sie über Systeme oder Geräte, die mit dem Internet verbunden sind (z. B. Überwachungskameras oder Gebäudesteuerungen), die ebenfalls mit Ihrem Geschäftsnetzwerk verbunden sind?

Diese Vermögenswerte können einen Weg in Ihre Geschäftsumgebung bieten, die ein Hacker verwenden könnte, um Ihre Daten zu stehlen oder zu beschädigen. Natürlich ist es wichtig zu wissen, welche Geräte und Systeme man besitzt. Einige Ihrer Vermögenswerte sind für den Geschäftsbetrieb wichtiger als andere, und ein vollständiges, aktuelles Inventar hilft Ihnen dabei, Prioritäten zu setzen, was auf welcher Ebene geschützt werden muss.

Wobei kann Ihnen diese Toolbox helfen?

Nach Umsetzung dieser Toolbox werden Sie Folgendes besser verstehen:

- ✔ **wie Sie eine Bestandsaufnahme Ihrer Daten und Systeme durchführen**
- ✔ **welche Geräte und Anwendungen für Ihren Geschäftsbetrieb entscheidend sind**

wie Sie die Toolbox verwenden

Verwenden Sie die Tools in der ***Kennen Sie Ihre eigene IT-Umgebung-Toolbox,*** um alle Ihre Geräte (einschließlich Desktops, Laptops, Smartphones und Druckern) und Anwendungen (z. B. E-Mail, Software, Webbrowser und Websites) zu identifizieren, damit Sie Maßnahmen zu deren Sicherung ergreifen können.

Dieses Inventar dient als Leitfaden und Checkliste für die Nutzung der weiteren Toolboxes. Stellen Sie sicher, dass Ihre Inventarliste immer auf dem neuesten Stand ist, besonders, wenn Sie neue Geräte, Konten oder wichtige Daten hinzufügen oder löschen.

Laden Sie die Tools von der Website herunter und notieren Sie sich den Zeitpunkt des Abschlusses. Nutzen Sie diese Gelegenheit, um eine regelmäßige Überprüfung zu planen, um sicherzustellen, dass alle Ihre Informationen auf dem neuesten Stand sind.

Navigieren in den Toolbox-Unterkategorien und zusätzlichen Informationen, die berücksichtigt werden sollen

1.1 Identifizieren Sie Ihre Geräte

Beim Erstellen eines Inventars ist es wichtig, alles in Ihrer Umgebung zu berücksichtigen.
Dazu gehören Elemente wie Desktops, Laptops, Smartphones, Drucker, Überwachungskameras, PoS, IoT-Geräte und Router.

Viele IoT-Geräte für Verbraucher verfügen über keine oder nur sehr minimale integrierte Sicherheit, also überlegen Sie, ob es möglich sein kann, sie vom Rest Ihres Netzwerks zu trennen oder sie vollständig zu entfernen.

Ältere Geräte sind möglicherweise nicht mehr unter Garantie und nicht mehr gegen neue Schwachstellen geschützt, sind aber für den Geschäftsbetrieb wichtig. Diese sollten als Teil Ihres Inventars identifiziert und ein Plan entwickelt werden, um sie entweder zu ersetzen, zu aktualisieren oder ihre Verwendung einzuschränken.

Viele Geräte wie Router, Überwachungskameras und Drucker werden manchmal vergessen, wenn man über die IT-Umgebung nachdenkt, aber alles, was eine Verbindung zum Internet oder zum lokalen Netzwerk hat, sollte bei der Bestandsaufnahme berücksichtigt werden, da diese Verbindungen oft einen potenziell einfachen Weg in Ihr Unternehmen darstellen.

Identifizieren Sie, wo sensible und geschäftskritische Daten aufbewahrt werden – sei es auf eigenständigen, netzwerkverbundenen Geräten oder in der Cloud. Es kann sein, dass zusätzliche Schutzniveaus für diese Geräte in Betracht gezogen werden sollten, aber Schritt eins besteht darin, zu dokumentieren, wo alles aufbewahrt wird.

1.2 Identifizieren Sie Ihre Anwendungen

Identifizieren Sie alle Ihre Anwendungen, einschließlich Geschäftsanwendungen, Online-Konten, für die Sie Ihre geschäftliche E-Mail-Adresse verwenden, und andere Anwendungen, auf die Sie entweder lokal oder remote über Ihre Geräte zugreifen.

Es ist wichtig, alle Anwendungen und Konten in Betracht zu ziehen und sich insbesondere an diejenigen zu erinnern, die Sie nicht mehr verwenden, da es unwahrscheinlich ist, dass Sie die Software für diese Anwendungen aktualisieren. Wenn sie Ihnen keinen Nutzen bieten, entfernen Sie sie oder schließen Sie die Konten. Ein altes Online-Konto kann einige Ihrer personenbezogenen Daten enthalten, und wenn die Organisation, für die Sie dieses Konto ursprünglich eingerichtet haben, verletzt wird, könnten Ihre Daten davon betroffen sein.

Weitere Informationen, Unterstützung und Anleitungen während der Implementierung finden Sie in der **Kategorie Kennen Sie Ihre eigene IT-Umgebung** im GCA Community Forum.

Link zu Kennen Sie Ihre eigene IT-Umgebung:

Toolkit: ***Toolbox Kennen Sie Ihre eigene IT-Umgebung***
https://gcatoolkit.org/de/kmu/kennen-sie-ihre-eigene-it-umgebung

Community Forum: Kategorie Kennen Sie Ihre eigene IT-Umgebung
https://community.globalcyberalliance.org/c/cybersecurity-toolbox/know-what-you-have/

Das Forum in anderen Sprachen
https://community.globalcyberalliance.org/t/language-support-on-the-forum-de-es-fr-id/900

Updates zur Abwehr

Welches Problem spricht diese Toolbox an?

Cyberkriminelle suchen nach Schwachstellen und Fehlern (bekannt als Verwundbarkeiten), die genutzt werden können, um Zugang zu Systemen zu erhalten oder bösartige Software zu verbreiten. Schädliche Akteure könnten sich Zugang zu den Finanzkonten Ihres Unternehmens, zu den Daten Ihrer Kunden und zu vielem mehr verschaffen. Sie können zum Schutz davor beitragen, indem Sie Ihre Verteidigung aktualisieren (d. h. Ihre Systeme, Geräte und Daten auf dem neuesten Stand halten). Hersteller und Softwareentwickler veröffentlichen regelmäßig Sicherheits-Updates für ihre Betriebssysteme und Anwendungen, um neu entdeckte Schwachstellen oder Sicherheitslücken zu beheben. Diese Korrekturen werden in der Regel als Patches bezeichnet, der Prozess heißt Patching.

Diese Toolbox trägt der Notwendigkeit Rechnung, diese Patches rechtzeitig anzuwenden, einschließlich der Einrichtung (auch als Konfiguration bezeichnet) von Systemen, damit sie, wann immer möglich, automatisch angewendet werden können. Darüber hinaus ist es wichtig zu erkennen, dass mit der Zeit viele Systeme hinzugefügt, angepasst oder umkonfiguriert werden, was zur Einführung von Schwächen führen kann, die von Cyberkriminellen ausgenutzt werden könnten. Ein weiterer Punkt, den Sie im Auge behalten sollten, ist die Frage, ob ein Drittanbieter Zugang zu den Daten in Ihren Systemen hat. Es ist wichtig, die Aufzeichnungen auf dem neuesten Stand zu halten; so können Sie die Updates verwalten, die notwendig sind, um sicherzustellen, dass die aktuellsten Patches auf Ihre Systeme, Geräte und Anwendungen angewendet werden.

Wobei kann Ihnen diese Toolbox helfen?

Nach Umsetzung dieser Toolbox werden Sie besser verstehen, wie Sie:

- ✔ **überprüfen, ob Sie die neueste Version der Software auf Ihrem Gerät ausführen**
- ✔ **Ihre Geräte so einstellen, dass Sicherheitsupdates automatisch akzeptiert und angewendet werden**
- ✔ **sichere Konfigurationseinstellungen für mobile Geräte, Webbrowser und Betriebssysteme implementieren**

Wie Sie die Toolbox verwenden

Verwenden Sie die Tools in der ***Updates zur Abwehr-Toolbox***, um sicherzustellen, dass Ihre Geräte und Anwendungen mit den neuesten Sicherheitspatches und mit den für die Art der enthaltenen Daten geeigneten Sicherheitsstufen ausgestattet sind. Wenn Sie ein Inventar in der Kennen Sie Ihre eigene IT-Umgebung-Toolbox erstellt haben, verwenden Sie diese als Leitfaden und Checkliste, um sicherzustellen, dass alle Ihre Geräte aktualisiert und so eingestellt sind, dass sie automatisch Sicherheitsupdates akzeptieren.

Wenn Sie die „Updates zur Abwehr-Toolbox“ abgeschlossen haben, aktualisieren Sie Ihre Sicherheits-Checkliste und setzen Sie eine Erinnerung, diesen Vorgang regelmäßig zu wiederholen, damit er zur Routine wird.

Erkunden der Toolbox-Unterkategorien und zusätzlichen Informationen, die berücksichtigt werden sollen

2.1 Aktualisieren Sie Ihre Geräte und Anwendungen

Wenn eine Lösung oder ein Patch für eine bekannte Schwachstelle entwickelt und veröffentlicht wird, ist es wichtig, dass alle Benutzer dieses Systems oder dieser Anwendung diese Patches sofort anwenden; idealerweise automatisch, denn bis dahin besteht die Gefahr, dass sie über diese Schwachstelle kompromittiert werden.

Überprüfen Sie jedes Gerät und jede Anwendung und konfigurieren Sie sie für die automatische Aktualisierung. Wir haben eine Liste der gebräuchlichsten Systeme und Anwendungen bereitgestellt, aber für diejenigen, die nicht in dieser Toolbox behandelt werden, sehen Sie sich die Anleitungen oder Supportseiten für das jeweilige Gerät oder die jeweilige Anwendung an. Haken Sie jedes Element auf der Liste ab. Diesen Schritt sollten Sie jedes Mal durchführen, wenn Sie neue Geräte oder Anwendungen in Ihrem Unternehmen einführen.

Häufig werden die sichersten Einstellungen nicht als Standard-Sicherheitseinstellung (als Konfiguration bezeichnet) für Ihre Geräte oder Anwendungen bereitgestellt, da Benutzerfreundlichkeit und Komfort Vorrang vor Sicherheit haben. Daher sollten Sie prüfen, ob es vom Hersteller empfohlene Sicherheitskonfigurationen für Ihre Geräte und Anwendungen gibt, und diese implementieren.

Alle Geräte, die nicht mehr unterstützt werden, sollten entfernt werden, da sie immer Gefahr laufen, durch eine neu entdeckte Schwachstelle beeinträchtigt zu werden. Wenn dies nicht möglich ist,

sollten sie von anderen Geräten isoliert und ihr Einsatz auf bestimmte Geschäftsfunktionen beschränkt werden.

Die in dieser Toolbox enthaltenen Tools bieten eine Konfigurationsanleitung für gängige Systeme zur automatischen Anwendung von Aktualisierungen. Sie sollten die Anleitung für alle Ihre Geräte und Systeme überprüfen, um sicherzustellen, dass sie entsprechend eingestellt sind.

2.2 Verschlüsseln Sie Ihre Daten

Wenn Ihr Computernetzwerk einen Einbruch erleidet, besteht eine hohe Wahrscheinlichkeit, dass der Hacker versucht, sensible oder vertrauliche Informationen zu stehlen, die er zu seinem eigenen finanziellen oder politischen Vorteil nutzen kann. Durch die Verschlüsselung von Daten, die auf Ihrer Festplatte gespeichert sind, wird es für Kriminelle viel schwieriger, diese Daten zu nutzen, da sie erst entschlüsselt werden müssen, bevor sie nutzbar sind.

Verschlüsselung ist der Prozess, bei dem Daten von einer lesbaren Form (d. h. Klartext) in eine codierte Form (d. h. Geheimtext) konvertiert werden. Diese Codierung ist so konzipiert, dass sie nur von Parteien gelesen werden kann, die den/die „Schlüssel“ zum Umkehren des Codierungsprozesses besitzen. Verschlüsselung ermöglicht die geheime Speicherung und Übermittlung von Daten und dient als Nachweis, dass diese von der Person stammen, die behauptet, sie gesendet zu haben.

Mit diesen Tools können Sie auf Ihrer Festplatte gespeicherte Dateien verschlüsseln. Wenn Ihr Betriebssystem hier nicht in der Toolbox enthalten ist, können weitere Optionen über den Gerätehersteller oder andere kommerziell erhältliche Sicherheitsangebote verfügbar sein.

2.3 Sichern Sie Ihre Websites

Für viele Unternehmen ist Ihre Website entscheidend für den Geschäftsbetrieb. Seine Nutzung kann den Fluss sensibler Informationen über die gesamte Lieferkette umfassen oder es kann die Haupthandelsplattform sein, auf die Ihr Unternehmen angewiesen ist. Sollten Hacker Zugriff auf die Website erhalten, könnten sie Daten abfangen oder stehlen, ihren Inhalt ändern, die Website mit Malware infizieren oder den Betrieb übernehmen. Jede dieser Maßnahmen könnte verheerende Auswirkungen auf die Handlungsfähigkeit Ihrer Organisation haben.

Hier finden Sie Tools, mit denen Sie Ihre Website regelmäßig überprüfen können (so genannte Scans), um Schwachstellen und potenzielle Schwächen zu identifizieren. Stellen Sie sicher, dass alle festgestellten Probleme von IT-kompetenten Mitarbeitern beurteilt und die entsprechenden Maßnahmen ergriffen werden.

Die Toolbox-Unterkategorien bieten Anleitungen und Tools für häufig verwendete Systeme. Für andere suchen Sie Hilfe über die Website des Anbieters oder bitten Sie um Rat im GCA Community Forum **Kategorie Updates zur Abwehr** oder in der **KMU-Community**.

Links zu Updates zur Abwehr:

Toolkit: ***Updates zur Abwehr-Toolbox***
https://gcatoolkit.org/de/kmu/updates-zur-abwehr

Community Forum: Kategorie Updates zur Abwehr
https://community.globalcyberalliance.org/c/cybersecurity-toolbox/update-your-defences/

KMU-Community
https://community.globalcyberalliance.org/c/community-discussions/small-business-community/

Mehr als ein sicheres Passwort

Welches Problem spricht diese Toolbox an?

Passwörter sind eine erste Verteidigungslinie zum Schutz Ihrer Konten und Daten (z. B. E-Mail, Personaldaten oder Kundendatenbanken).

Leider sind Passwörter oft ein leichtes Ziel für Cyberkriminelle, und hackbezogene Datenverletzungen entstehen oft aufgrund von schwachen Passwörtern. Angreifer haben viele Möglichkeiten, auf Ihre Passwörter zuzugreifen, von leicht erhältlichen Passwort-Crackern, d. h. Programmen, die häufig verwendete Kombinationen durchlaufen, bis hin zur Verwendung eines Benutzernamens und eines Passworts, die von einem Konto stammen, das einen Sicherheitsverstoß erlitten hat, indem sie diese auf anderen beliebten Websites ausprobieren. Diese Techniken erfordern wenig technische Fähigkeiten, sind schnell, voll automatisiert und für diejenigen, die wissen, wo sie im Internet zu finden sind, leicht zugänglich. Ein weiteres Problem für kleine und mittlere Unternehmen besteht darin, dass viele von ihnen keine Richtlinie für Passwörter haben oder, falls sie eine haben, diese nicht strikt durchsetzen.

Sichere Passwörter sind daher zum Schutz Ihrer Daten unerlässlich. Aber Sie müssen noch einen Schritt weiter gehen, indem Sie eine Zwei- oder Mehr-Faktor-Authentifizierung (2FA) implementieren.

2FA erfordert mehrere Anmeldedaten, wodurch es für einen Angreifer viel schwieriger wird, Zugang zu Ihren Konten zu erhalten.

Bei 2FA benötigt ein Benutzer Folgendes:

- Etwas, das Sie kennen, z. B. ein Passwort;
- Und etwas, das Sie haben, wie ein Token (Google Authenticator, Authy, Okta, RSA etc.) oder einen Verifizierungscode, der an Ihr Handy gesendet wird; oder
- Etwas, das Sie verkörpern, wie Ihr Fingerabdruck oder Gesicht (Biometrie).

Diese Toolbox hilft Ihnen bei der Erstellung von stärkeren, eindeutigen Passwörtern für jedes Ihrer Konten und zeigt Ihnen, wie Sie 2FA einrichten; beides wichtige Schritte zum Schutz des Zugriffs auf Ihre Konten und Daten.

Wobei kann Ihnen diese Toolbox helfen?

Nach Umsetzung dieser Toolbox werden Sie besser verstehen, wie Sie:

- ✔ **Beim Erstellen eines sicheren Passworts**
- ✔ **Beim Testen Ihrer Konten, um festzustellen, ob sie beeinträchtigt wurden**
- ✔ **Beim Einrichten von 2FA für die gängigsten Online-Konten**

Wie Sie die Toolbox verwenden

Verwenden Sie die Tools in der ***Mehr als ein sicheres Passwort-Toolbox,*** um sicherzustellen, dass Ihre Geräte und Anwendungen mit starken Passwörtern und 2FA eingerichtet sind. Wenn Sie ein Inventar in Kennen Sie Ihre eigene IT-Umgebung erstellt haben, verwenden Sie dieses als Leitfaden und Checkliste, um sicherzustellen, dass Sie es in allen Ihren Konten implementiert haben.

Wenn Sie die „Mehr als ein sicheres Passwort-Toolbox“ abgeschlossen haben, aktualisieren Sie Ihre Sicherheits-Checkliste und setzen Sie eine Erinnerung, diesen Vorgang regelmäßig zu wiederholen, damit er zur Routine wird.

Erkunden der Toolbox-Unterkategorien und zusätzlichen Informationen, die berücksichtigt werden sollen

3.1 Sichere Passwörter

Eine der häufigsten Methoden, wie sich Kriminelle Zugriff auf Ihre Konten, Ihr Netzwerk und Ihre Daten verschaffen, ist die Anmeldung unter falscher Identität. Es ist wirklich wichtig, dass Sie:

- für jedes Ihrer Konten ein eindeutiges, sicheres Passwort (oder eine Passphrase) verwenden.
- Buchstaben, Zahlen und Sonderzeichen verwenden, um ein sicheres Passwort sicherzustellen.
- Ihr Passwort sofort ändern, wenn Sie gestohlen wurden.
- Ihre Passwörter geheim und sicher sind.
- niemals ein Passwort wiederverwenden.
- niemals auf einen Link in einer E-Mail klicken, in der Ihnen mitgeteilt wird: „Es ist Zeit, Ihr Passwort zurückzusetzen“; immer über den Webbrowser auf die Konto-Website zugreifen.
- die Anmeldung bei Konten über öffentliches WLAN vermeiden.

Die Verwendung desselben Passworts für mehrere Konten bedeutet, dass ein Krimineller, wenn er eines Ihrer Passwörter erhält, effektiv Zugang zu allen Ihren Konten erhalten hat, die es verwenden. Benutzername und Passwortdaten können von Kriminellen, die sie in einem Cyberangriff gestohlen haben, online verkauft und wieder verwendet werden, bis das Passwort geändert wird. Schneller technologischer Fortschritt bedeutet, dass ein billiger, moderner Laptop schnell alle Kombinationen durchlaufen kann, um kurze, einfache Passwörter auszuarbeiten.

Sie sollten über eine Richtlinie für Passwörter verfügen, die von allen Mitarbeitern und Auftragnehmern, die Zugang zu Ihren Systemen haben, verstanden und befolgt wird. Einige Systeme und Anwendungen können es Ihnen ermöglichen, ein minimal zulässiges Passwort zu erzwingen, so dass es sich sicherlich lohnt, dies in den Sicherheitseinstellungen zu überprüfen.

Sie können die Tools in Sichere Passwörter verwenden, um mehr über Passwörter zu erfahren und um zu überprüfen, ob Ihre E-Mail-Adresse bei einem Verstoß gestohlen wurde. Wenn dies der Fall ist, dann ändern Sie Ihr Passwort sofort und verwenden Sie niemals Passwörter erneut.

Denken Sie auch daran, die Passworteinstellungen auf Routern, Druckern und anderen an Ihr Netzwerk angeschlossenen Geräten zu überprüfen. Diese können leicht vergessen werden und werden in der Regel mit einfachen Standardpasswörtern ausgeliefert. Arbeiten Sie das Inventar, das Sie in Kennen Sie Ihre eigene IT-Umgebung erstellt haben, durch und haken Sie es nach und nach ab!

3.2 Tools für die 2FA

Die Zwei-Faktor-Authentifizierung (2FA) bietet neben den Passwörtern eine wichtige zweite Verteidigungslinie, um Konten vor unbefugtem Zugriff zu schützen. Es gibt eine Reihe von verschiedenen Authentifizierungsmethoden, die für 2FA verwendet werden können. Diese reichen von einem einzigartigen Code, der per Text an Ihr Mobiltelefon geschickt wird, über einen Hardware-Token, den Sie mit sich herumtragen, bis hin zu einem Fingerabdruck oder einer Gesichtserkennung.

Tools für 2FA enthalten herunterladbare Ressourcen, die akzeptierte Authentifizierungsmethoden für viele gängige Konten bieten.

Berücksichtigen Sie bei der Implementierung der Tools und Anleitungen in der Mehr als ein sicheres Passwort-Toolbox auch, welche Berechtigungen jeder Benutzer beim Zugriff auf geschäftsbezogene Anwendungen hat. Ziehen Sie in Betracht, den Zugang nur auf diejenigen zu beschränken, die ihn benötigen, und zwar in dem Maße, wie es ihre Rolle erfordert.

3.3 Verwalten Sie Ihre Passwörter

Passwort-Manager sind eine Möglichkeit, alle Ihre Passwörter sicher zusammen zu halten, ohne sich jedes einzelne einzeln merken zu müssen. Das bedeutet, dass Sie sich jedes Mal nur ein Passwort merken müssen, wenn Sie sich bei einem der Konten anmelden wollen, dessen Passwort im Passwort-Manager gespeichert ist. Passwort-Manager sind praktischer. Es bedeutet aber auch, dass bei einer Kompromittierung des Passwort-Managers der Angreifer Zugriff auf alle Passwörter hätte.

Weitere Informationen, Unterstützung und Anleitungen während der Implementierung finden Sie in der **Kategorie Mehr als ein sicheres Passwort** im GCA Community Forum.

Links zu Mehr als ein sicheres Passwort:

Toolkit: ***Mehr als ein sicheres Passwort-Toolbox***
https://gcatoolkit.org/de/kmu/mehr-als-ein-sicheres-passwort

Community-Forum: Kategorie Mehr als ein sicheres Passwort
https://community.globalcyberalliance.org/c/cybersecurity-toolbox/beyond-simple-passwords/

Verhindern von Phishing und Malware

Welches Problem spricht diese Toolbox an?

Jedes Jahr fallen viele kleine Unternehmen kostspieligen Malware- und Phishing-Angriffen zum Opfer. Wenn ein Benutzer auf eine mit Malware infizierte Website klickt oder einen

infizierten Anhang in einer Phishing-E-Mail öffnet, kann das Ergebnis das Löschen oder Ändern von Dateien, veränderte Anwendungen oder deaktivierte Systemfunktionen sein.

Malware ist jede Software, die darauf ausgelegt ist, Schäden an und/oder unbefugten Zugriff auf Geräte oder Netzwerke zu verursachen. Phishing-E-Mails täuschen dem Benutzer vor, dass er es mit einem vertrauenswürdigen Unternehmen zu tun hat, so dass sich der Angreifer unbefugten Zugang zu privaten, sensiblen, eingeschränkten Inhalten oder Geld verschaffen kann. Der Angreifer tut alles, was er kann, um seine E-Mail echt und verlockend erscheinen zu lassen, damit der Benutzer sie anklicken oder öffnen kann. Die E-Mails können so aussehen, als kämen sie von jemandem, den Sie kennen, sie könnten die Logos und das Format von E-Mails bekannter Organisationen nachahmen, oder sie könnten sich auf aktuelle Schlagzeilen oder eine Arbeit beziehen, die Sie gerade gemacht haben.

Einige Schätzungen gehen davon aus, dass mehr als 90 % der Cyberattacken mit einer Phishing-E-Mail beginnen. Wenn Sie auf den Link klicken oder den Anhang in einer Phishing-E-Mail öffnen, können Sie eine beliebige Anzahl von Aktivitäten auslösen, die der Angreifer eingerichtet hat, z. B. den Diebstahl Ihrer Daten, die Einrichtung einer Geheimroute (einer so genannten Hintertür oder Backdoor) in Ihren Computer zur späteren Verwendung, die Installation einer Art von Malware, durch die der Angreifer Sie von Ihren Daten aussperrt und von Ihnen Lösegeld für den Zugriff verlangt (so genannte Ransomware), oder das Herunterladen einer anderen Art von Malware, die es dem Angreifer ermöglicht, Ihre Eingaben zu sehen, z. B. Passwörter oder Kontonummern (so genannte Spyware).

Die Folgen von Phishing- und Malware-Angriffen sind für kleine Unternehmen schwerwiegend. Zu den Auswirkungen können Datenverlust oder -beschädigung, Einkommensverluste, wenn Ihr Unternehmen während eines Angriffs stillgelegt wird, Ausgaben für die Reparatur/Ersetzung von Geräten, Kosten für die Benachrichtigung von Kunden oder Klienten über einen Verstoß sowie Rufschädigung und potenzielle Klagen gehören.

Die ***Verhindern von Phishing und Malware-Toolbox*** hilft Ihnen, Risiken zu reduzieren, indem Sie Ihre Widerstandsfähigkeit gegenüber Angriffen stärken. Dazu gehören Tools, die verhindern, dass Sie auf infizierte Websites gehen, Antiviren-Software, die das Eindringen von Viren und anderer Malware in Ihre Systeme verhindert, und Anzeigenblocker, die Online-Werbung verhindern, die Viren übertragen kann.

Wobei kann Ihnen diese Toolbox helfen?

Nach Umsetzung dieser Toolbox werden Sie Folgendes besser verstehen:

- ✔ **Wie Antiviren-Software Ihre Systeme und Daten schützt**

- ✔ **So installieren Sie Antiviren-Software auf Ihrem System**
- ✔ **Digitale Werbung und die Risiken, die sie birgt**
- ✔ **So installieren Sie einen Anzeigenblocker, um Pop-ups-Anzeigen, Videos und andere unerwünschte Inhalte zu sperren**
- ✔ **Was DNS bedeutet und warum es wichtig ist**
- ✔ **Funktionsweise der DNS-Sicherheit und welche Arten von Angriffen sie mindern**
- ✔ **So installieren Sie Quad9 auf Ihren Android-Geräten und -Computern**

Navigieren in den Toolbox-Unterkategorien und zusätzlichen Informationen, die berücksichtigt werden sollen

Die Werkzeuge wurden sorgfältig auf der Grundlage anerkannter globaler Standards ausgewählt und werden hier nicht in einer bestimmten Reihenfolge oder empfohlenen Priorität dargestellt.

4.1 Antivirenschutz

Es ist wichtig, einen Echtzeit-Antivirenschutz zu verwenden, da dieser in Echtzeit auf Viren prüft und so Viren entfernt werden, bevor sie Schaden anrichten können, und er wird aktualisiert, sobald ein neuer Virenschutz entwickelt wird.

4.2 Anzeigenblocker

Einige Online-Werbungen oder Nachrichten, die beim Surfen auf einer Website angezeigt werden, sind nützlich; andere können jedoch schädlichen Code enthalten und Ihren Computer mit Malware infizieren, wenn Sie auf die Anzeige klicken. Ein Anzeigenblocker kann verwendet werden, um zu verhindern, dass Anzeigen auf Webseiten erscheinen, was zusätzlichen Schutz beim Surfen bietet.

4.3 DNS-Sicherheit

Die DNS-Sicherheit verwendet das Domain Name System (das Internet-Äquivalent eines Telefonbuchs), um den textbasierten Website-Namen (Domain-Name), den ein Benutzer im Browser eingibt, in eine eindeutige Zahlenmenge (IP-Adresse) zu übersetzen, die von Computern verstanden wird.

Viele Angreifer nutzen gleich aussehende Website-Domänennamen, um Opfern den Eindruck zu vermitteln, sich mit einer legitimen Website zu verbinden. Diese Seiten können wie der echte Website-Name aussehen, aber eine genauere Betrachtung kann Unterschiede zeigen.

So könnte z. B. die URL einer legitimen Website eines Unternehmens folgendermaßen aussehen: „www.mygreatwidgets.com“, aber die gefälschte könnte wie folgt aussehen: „www.rnygreatwidgets.com."

DNS-Firewalls, die eine Art der DNS-Sicherheit darstellen, können dazu beitragen, Viren und Phishing-Angriffe zu verhindern, da sie prüfen, ob die IP-Adresse der angeforderten Website bekanntermaßen bösartigen Code beherbergt, und wenn dies der Fall ist, den Zugang zu ihr sperren. Benutzer können DNS-Filter-Services auf ihren Systemen implementieren, indem sie die Tools innerhalb dieser Unterkategorie verwenden, um den Zugriff auf bekannte bösartige Websites zu verhindern.

Die Toolbox-Unterkategorien bieten Werkzeuge für häufig verwendete Systeme. Für weiteren Support suchen oder fragen Sie im GCA Community Forum **Kategorie Verhindern von Phishing und Malware** oder in der **KMU-Community**.

Links für Verhindern von Phishing und Malware:

Toolkit: ***Toolbox zum Verhindern von Phishing und Malware***
https://gcatoolkit.org/de/kmu/verhindern-von-phishing-und-malware/

Community-Forum: Kategorie Verhindern von Phishing und Malware
https://community.globalcyberalliance.org/c/cybersecurity-toolbox/prevent-phishing-and-viruses/

KMU-Community
https://community.globalcyberalliance.org/c/community-discussions/small-business-community/

Backup und Wiederherstellung

Welches Problem spricht diese Toolbox an?

Der Verlust oder die Verfälschung von Daten könnte auf einen Cyberangriff (z. B. Ransomware) oder auf Geräteversagen oder -diebstahl, menschliches Versagen, versehentliche Beschädigungen, Feuer oder Überschwemmung zurückzuführen sein. Unabhängig von der Ursache können die Auswirkungen von Datenverlusten oder Geräteausfallzeiten die Produktivität und Rentabilität Ihres Unternehmens ernsthaft beeinträchtigen.

Eine Sicherheitskopie ist eine Kopie Ihrer Daten, die an einem anderen Ort als die Originaldaten gespeichert wird und Ihnen bei der Wiederherstellung nach einem Angriff oder Datenverlust helfen

kann. Regelmäßige On- und Offline-Backups erleichtern eine schnellere Wiederherstellung nach Datenverlust oder Datenbeschädigung. Beides ist wichtig, weil Online-Backups so eingestellt sind, dass sie automatisch über ein Netzwerk gesichert werden, während Offline-Backups das Anschließen und Entfernen eines externen Geräts (z. B. eines USB-Sticks oder einer Festplatte) zur physischen Speicherung an einem anderen Ort erfordern (was auch gegen die versehentliche Sicherung bereits beschädigter Daten hilft).

Wobei kann Ihnen diese Toolbox helfen?

Nach Umsetzung dieser Toolbox werden Sie Folgendes besser verstehen:

- ✔ **Warum Backups für Ihr Unternehmen wichtig sind, insbesondere bei der Wiederherstellung nach einem Ransomware-Angriff**
- ✔ **Wie Sie ein vollständiges Backup auf Ihrem Windows- oder Mac-Rechner aktivieren**

Wie Sie die Toolbox verwenden

Verwenden Sie die Tools in der ***Backup- und Wiederherstellungs-Toolbox***, um sicherzustellen, dass Ihre Systeme regelmäßig gesichert werden, und zwar in einer Höhe und Häufigkeit, die der Art der darin enthaltenen Daten entspricht.

Was sollten Sie sichern? Das hängt von Ihren Informationen und dem Risiko für den Verlust dieser Informationen ab. Wenn Sie ein Inventar in der Kennen Sie Ihre eigene IT-Umgebung-Toolbox erstellt haben, verwenden Sie diese als Leitfaden und Checkliste, um es laufend zu aktualisieren.

Sobald Sie die Backup- und Wiederherstellungs-Toolbox abgeschlossen haben, aktualisieren Sie Ihre Sicherheits-Checkliste und legen Sie eine Erinnerung fest, die Sie regelmäßig überprüfen müssen, um sicherzustellen, dass Ihre Richtlinie für Ihr Unternehmen angemessen bleibt.

Navigieren in den Toolbox-Unterkategorien und zusätzlichen Informationen, die berücksichtigt werden sollen

Ransomware ist eine Angriffsmethode, die für KMU zu einem ernsthaften Problem geworden ist. Ransomware ist eine Art von bösartiger Software, die Computer infiziert und den Zugang zu Daten blockiert. Der Täter verlangt die Zahlung, manchmal in Form von Kryptogeld (d. h. Bitcoin, das weniger leicht zurückzuverfolgen ist als herkömmliche Überweisungen), mit dem Versprechen, dass die Daten wiederhergestellt werden, sobald das Lösegeld eingegangen ist. Sicherungen Ihrer Daten

sind ein wichtiger Schutz für den Zugriff auf Ihre Informationen, wenn Sie Opfer von Ransomware geworden sind.

5.1 Backups nach Betriebssystem

Eine solide Richtlinie für Backups, die sowohl On- als auch Offline-Backups umfasst, erleichtert eine schnellere Wiederherstellung nach Datenverlust oder Datenbeschädigung.

- Die verschiedenen Datensätze, die Sie in Ihrem Besitz haben, sollten innerhalb des Inventars kategorisiert werden (siehe die Kennen Sie Ihre eigene IT-Umgebung-Toolbox für Hilfe bei der Erstellung eines Inventars).
- Ziehen Sie die Verwendung von Verschlüsselung für sensible Informationen in Betracht (weitere Informationen zur Verschlüsselung finden Sie in der „Updates zur Abwehr-Toolbox").
- Implementieren Sie einen vernünftigen Ansatz zur Sicherung der einzelnen Datensätze unter Berücksichtigung der „Verlustauswirkungen“ für jeden einzelnen Datensatz. Der Schaden kann rufschädigend, finanziell oder rechtlich sein.

In der Unterkategorie Backup Operating Systems finden Sie Anleitungen für Backups auf gängigen Betriebssystemen. Falls Ihre nicht dabei ist, suchen Sie Hilfe über die Website Ihres Anbieters oder fragen Sie in der Kategorie Backup und Wiederherstellung im GCA Community Forum nach.

Stellen Sie außerdem sicher, dass Sie über einen Notfallwiederherstellungsplan verfügen, der die Wiederherstellung kritischer Systeme nach einer Katastrophe (sei es ein Unfall oder eine Naturkatastrophe) ermöglicht. Ein Plan trägt dazu bei, die Wiederherstellungszeit und Schäden an den Systemen zu minimieren, schützt vor möglichen Haftungsansprüchen und kann auch die Sicherheit verbessern. Es gibt viele Vorlagen und Leitfäden für die Entwicklung eines Plans, die online verfügbar sind. Halten Sie den Plan auf dem Laufenden und führen Sie Simulationsszenarien durch, um den Plan zu üben und sicherzustellen, dass alle wissen, wie er umzusetzen ist.

Links zu Backup und Wiederherstellung:

Toolkit: *Backup- und Wiederherstellungs-Toolbox*
https://gcatoolkit.org/de/kmu/backup-und-wiederherstellung/

Community-Forum: Forum Backup und Wiederherstellung
https://community.globalcyberalliance.org/c/cybersecurity-toolbox/back-up-and-recover/

Schutz Ihrer E-Mails und Ihres Rufs

Welches Problem spricht diese Toolbox an?

E-Mail wird oft als Ausgangspunkt für einen Cyberangriff verwendet. Es geht extrem schnell und ist kostengünstig, Tausende von E-Mails an ahnungslose Empfänger zu versenden, in der Hoffnung, dass zumindest einige von ihnen diese als echt erachten und auf den schädlichen Website-Link klicken oder den bösartigen Anhang herunterladen.

Eine der Techniken, die Cyberkriminelle verwenden, besteht darin, die E-Mail so aussehen zu lassen, als sei sie von einer legitimen Quelle, wie z. B. Ihrem Finanzinstitut, einem Kunden, einem Geschäftspartner oder einer anderen bekannten Organisation, gesendet worden. Eine dieser Techniken ist als E-Mail-Domain-Spoofing bekannt, bei dem die verwendete „gefälschte“ E-Mail-Adresse genau der echten entspricht, so dass es so aussieht, als wäre sie tatsächlich von dieser Organisation gesendet worden, so dass der Empfänger wenig Grund zu der Annahme hat, dass sie nicht tatsächlich von ihr gesendet wurde.

Wenn Ihre Firmen-E-Mail-Domain (der Teil Ihrer E-Mail-Adresse nach dem „@") gefälscht ist, könnte dies schwerwiegende Folgen für Sie, Ihre Kunden und die Lieferkette haben. Wenn dieser E-Mail-Empfänger aufgrund der E-Mail etwas unternommen hat, weil er wirklich glaubte, dass sie von Ihnen kam, könnte dies dazu führen, dass sein Computersystem mit einer Form von Malware oder Ransomware infiziert wird. Außerdem kann der Kriminelle möglicherweise die Kontrolle über Ihre Systeme übernehmen und Ihre Bankdaten manipulieren, sodass Kunden Zahlungen unbemerkt auf andere Konten vornehmen.

Die Schutz Ihrer E-Mails und Ihrer Marke-Toolbox bietet Anleitungen und Tools zum Schutz vor dieser Art von Bedrohung, einschließlich einer Anleitung zur Verwendung eines E-Mail-Standards, der als DMARC (Domain-based Authentication, Reporting, and Conformance) bekannt ist. DMARC ist eine effektive Möglichkeit, Spammer und Phisher daran zu hindern, Unternehmensdomänen für gefährliche Cyberangriffe zu verwenden. Dabei wird überprüft, ob der Absender einer E-Mail berechtigt ist, Ihre E-Mail-Domäne zu nutzen und E-Mails zu senden.

Angreifer können auch „Doppelgänger“-Websites einrichten. Beispielsweise kann die echte Domain „BestBusiness.com“ durch die Registrierung von „BestBusness.com“ oder „BestBusiness.net“ verkörpert werden, um Kunden oder Benutzer dazu zu verleiten, sie zu besuchen.

Wenn Ihre E-Mail- oder Website-Domains gefälscht werden, kann dies zu einer Schädigung Ihres Rufs und Ihrer Marke sowie zu einem Schaden für Ihre Kunden führen. Der Einsatz der Tools im Schutz Ihrer E-Mails und Ihrer Marke-Toolkit hilft, Identitätswechsel zu erkennen und zu verhindern.

Wobei kann Ihnen diese Toolbox helfen?

Nach Umsetzung dieser Toolbox werden Sie Folgendes besser verstehen:

- ✔ **Was DMARC bedeutet, warum es wichtig ist und welche Angriffe es entschärft**
- ✔ **Das DMARC-Einrichtungshandbuch**
- ✔ **, wie Sie Ihre eigene E-Mail-Domäne überprüfen, um festzustellen, ob DMARC aktiviert ist**

Wie Sie die Toolbox verwenden

Verwenden Sie die Tools der ***Schutz Ihrer E-Mails und Ihrer Marke-Toolbox***, um sicherzustellen, dass Ihr Unternehmen durch die Implementierung von DMARC vor E-Mail-Domain-Spoofing geschützt ist, und identifizieren Sie potenzielle ähnliche Website-Domains.

Aktualisieren Sie Ihre Sicherheits-Checkliste, sobald sie vollständig ist, und ermutigen Sie Ihre Kunden und Ihre Lieferkette, die ihre eigene Domäne verwenden, dies ebenfalls zu tun, da die Wirksamkeit von DMARC davon abhängt, dass sowohl der Absender als auch der Empfänger DMARC implementiert haben.

Navigieren in den Toolbox-Unterkategorien und zusätzlichen Informationen, die berücksichtigt werden sollen

6.1 DMARC implementieren

Verwenden Sie die Tools in dieser Unterkategorie, um mehr über DMARC zu erfahren, und überprüfen Sie, ob Ihre E-Mail-Domain durch DMARC geschützt ist und wenn ja, bis zu welchem Grad.

6.2 DMARC-Berichte verstehen

Sobald eine DMARC-Richtlinie auf Ihrer E-Mail-Domain eingerichtet ist, werden Sie Berichte erhalten, die zeigen, wie Ihre E-Mail-Domain genutzt wird. Diese können in ihrem Rohformat schwer zu unterbrechen sein.

Die Tools in der Unterkategorie „DMARC-Berichte verstehen“ helfen bei der Interpretation und schnelleren Identifizierung von betrügerischen Aktivitäten. Auf diese Weise können Sie mit Zuversicht die Ebenen der Richtlinien von „keine“ über „Quarantäne“ bis hin zur höchsten Ebene der „Ablehnung“ durchlaufen. Es ist wichtig, auch alle E-Mail-Organisationen oder Services in Betracht zu ziehen, die berechtigt sind, in Ihrem Namen E-Mails zu versenden, wie z. B. E-Mail-Marketing-Services, und zu prüfen, ob sie DMARC implementiert haben.

Erst wenn Ihre E-Mail-Domain auf „Ablehnung“ steht, wird der volle Nutzen von DMARC realisiert.

6.3 Markenschutz

Betrüger können Domains registrieren, die Ihrer eigenen Domain sehr ähnlich sehen, in der Hoffnung, dass die Leute sich an sie anklicken. Verwenden Sie die Tools hier, um Domains zu identifizieren, die versuchen, Ihre zu imitieren, sowie Domains, die Phishing oder bösartige Inhalte enthalten, die auf Ihre Domain abzielen.

Weitere Unterstützung bei der Implementierung von DMARC erhalten Sie im **DMARC-Forum** oder in der **Kategorie Schutz Ihrer E-Mails und Ihrer Marke** im GCA Community-Forum.

Links zu Schutz Ihrer E-Mails und Ihrer Marke:

Toolkit: ***Schutz Ihrer E-Mails und Ihrer Marke-Toolbox***
https://gcatoolkit.org/de/kmu/schutz-ihrer-e-mails-und-ihrer-marke/

Community-Forum: DMARC Forum
https://community.globalcyberalliance.org/c/dmarc/

Kategorie Schutz Ihrer E-Mails und Ihrer Marke
https://community.globalcyberalliance.org/c/cybersecurity-toolbox/protect-your-email-and-reputation

Glossar

Ein Glossar einiger häufig verwendeter Begriffe im Zusammenhang mit Cybersicherheit. Einige dieser Begriffe wurden in die Kapitel des Handbuchs zum GCA-Cybersicherheits-Toolkit für KMU aufgenommen, während andere für zusätzliche Informationen zur Verfügung gestellt werden, falls Sie sich auf eigene Faust weiter informieren möchten.

Konto Bezieht sich im Allgemeinen auf den Zugriff auf ein Computersystem oder einen Onlinedienst, der in der Regel ein Passwort erfordert.

Gegner Eine Person, Gruppe, Organisation oder Regierung, die schädliche Aktivitäten durchführt oder beabsichtigt.

Antivirenschutz Software, die darauf ausgelegt ist, Viren und andere Arten von bösartiger Software zu erkennen, zu stoppen und zu entfernen.

Anwendung (App) Ein Programm, das für die Ausführung bestimmter Aufgaben entwickelt wurde. App bezieht sich oft auf Programme, die auf mobile Geräte heruntergeladen werden.

Asset bzw. Eigentum/Vermögenswert Eine Person, Struktur, Einrichtung, Informationen und Aufzeichnungen, IT-Systeme und Ressourcen, Material, Prozess, Beziehungen oder Reputation, die einen Wert hat. Alles Nützliche, das zum Erfolg von etwas beiträgt, wie z. B. eine organisatorische Mission; Vermögenswerte sind Werte oder Eigenschaften, denen Wert zugeordnet werden kann.

Angriff Ein Versuch, unberechtigten Zugriff auf Systemdienste, Ressourcen oder Informationen zu erlangen, oder der Versuch, die Systemintegrität zu gefährden. Die absichtliche Handlung des Versuchs, einen oder mehrere Sicherheitsdienste oder Kontrollen eines Informationssystems zu umgehen.

Angriffssignatur Ein charakteristisches oder unverwechselbares Muster, nach dem gesucht werden kann oder das zum Abgleichen zuvor identifizierter Angriffe verwendet werden kann.

Angriffsfläche Der Satz von Möglichkeiten, wie ein Gegner in ein System eindringen und möglicherweise Schaden anrichten kann. Die Eigenschaften eines Informationssystems, die es einem Gegner erlauben, das Informationssystem zu sondieren, anzugreifen oder seine Präsenz im Informationssystem aufrechtzuerhalten.

Angreifer Schädlicher Akteur, der versucht, Computersysteme mit der Absicht auszunutzen, ihre Informationen zu ändern, zu zerstören, zu stehlen oder zu deaktivieren und dann das Ergebnis auszunutzen.

Authentifizierung Der Prozess zum Überprüfen, ob jemand derjenige ist, der nach seinen Angaben beim Zugriff auf einen Computer oder Onlinedienst vorliegt. Auch die Quelle und Integrität von Daten, Benutzer, Prozess oder Gerät.

Hintertür bzw. Backdoor Eine verdeckte Möglichkeit für Cyberkriminelle, unberechtigten Zugriff auf ein Computersystem zu erlangen

Sicherheitskopie bzw. Backup Eine Kopie Ihrer Daten, die an einem anderen Ort als die Originaldaten gespeichert wird und Ihnen bei der Wiederherstellung nach einem Angriff oder Datenverlust helfen kann.

Sichern Erstellen einer Kopie der auf einem Computer oder Server gespeicherten Daten, um die potenziellen Auswirkungen von Fehlern oder Verlusten zu mindern.

Bot Ein Computer oder ein Gerät, das mit dem Internet verbunden ist und heimlich mit bösartigem Code kompromittiert wurde, um Aktivitäten unter dem Befehl und der Kontrolle eines Remoteadministrators auszuführen.

Botnet Ein Netzwerk infizierter Geräte (Bots), die mit dem Internet verbunden sind, wird verwendet, um koordinierte Cyberangriffe ohne Wissen ihres Besitzers zu begehen.

Verstoß Ein Vorfall, bei dem auf Daten, Computersysteme oder Netzwerke auf nicht autorisierte Weise zugegriffen wird oder bei dem Daten, Computersysteme oder Netzwerke betroffen sind.

Brute-Force-Angriff Verwendung einer Datenverarbeitungseinheit, um automatisch eine große Anzahl von Werten einzugeben, in der Regel, um Passwörter zu entdecken und Zugriff zu erhalten.

Fehler bzw. Bug Ein unerwarteter und relativ kleiner Defekt, Fehler, Mangel oder Unvollkommenheit in einem Informationssystem oder Gerät.

Konfiguration Die Anordnung von Software- und Hardwarekomponenten eines Computersystems oder -geräts.

Konfigurieren Der Prozess der Einrichtung von Software oder Geräten für einen bestimmten Computer, ein bestimmtes System oder eine Aufgabe

Cyberangriff Schädliche Versuche, Computersysteme, Netzwerke oder Geräte über Cyber-Mittel zu beschädigen, zu unterbrechen oder unberechtigten Zugriff zu erlangen.

Cyber-Vorfall Ein Verstoß gegen die Sicherheitsregeln für ein System oder einen Dienst, am häufigsten Versuche, unberechtigten Zugriff auf ein System und/oder Daten, unbefugte Nutzung von Systemen für die Verarbeitung oder Speicherung von Daten, Änderungen an einer System-Firmware-Software oder -Hardware ohne Zustimmung der Systembesitzer, schädliche Störungen und/oder Denial-of-Service zu erhalten.

Cybersicherheit Der Schutz von Geräten, Diensten und Netzwerken – und deren Informationen – vor Diebstahl oder Beschädigung.

Kryptowährung digitales Geld. Kryptowährung wird in einer digitalen Brieftasche (auch Wallet genannt) (online, auf Ihrem Computer oder auf anderer Hardware) gespeichert. Kryptowährung wird in der Regel nicht von einer Regierung unterstützt und hat somit nicht den gleichen Schutz wie Geld, das in einer Bank gespeichert ist.

Wörterbuchangriff Eine Art *Brute-Force-Angriff,* bei dem der Angreifer bekannte Wörter, Ausdrücke oder allgemeine Passwörter zum Erraten verwendet.

Digitaler Fußabdruck Ein „Fußabdruck“ digitaler Informationen, die die Online-Aktivitäten eines Benutzers hinterlassen.

Denial-of-Service (DoS) Ein Angriff, bei dem legitimen Benutzern der Zugriff auf Computerdienste (oder Ressourcen) verweigert wird, in der Regel durch Überladen des Dienstes mit Anforderungen.

Gerät Eine Computerhardware, die für eine bestimmte Funktion entwickelt wurde, z. B. Laptop, Mobiltelefon oder Drucker.

DMARC bedeutet Domain-based Message Authentication, Reporting and Conformance. DMARC ist ein Mechanismus, der es Absendern und Empfängern ermöglicht, ihre Domain vor betrügerischen E-Mails zu überwachen und zu verbessern.

E-Mail-Domain-Spoofing Eine Technik, die von Cyberkriminellen verwendet wird, bei der die „gespoofte“ E-Mail-Adresse genau die gleiche ist wie die echte, so dass sie tatsächlich von dieser Organisation gesendet worden zu sein scheint.

Verschlüsselung Konvertieren von Daten in ein Formular, das von Unbefugten nicht leicht verstanden werden kann.

Firewall Ein Hardware-/Softwaregerät oder ein Softwareprogramm, das den Netzwerkverkehr gemäß einer Reihe von Regeln begrenzt, welche Zugriffe erlaubt oder nicht autorisiert sind.

Hacker Jemand, der die Computersicherheit aus schädlichen Gründen, Ansehen oder persönlichen Gewinn verletzt

Hardware Ein Computer, seine Komponenten und seine zugehörigen Geräte. Die Hardware umfasst Festplattenlaufwerke, integrierte Schaltungen, Bildschirme, Kabel, Modems, Lautsprecher und Drucker.

(Interne) Insider-Bedrohung Eine Person oder Gruppe von Personen mit Zugang und/oder Insiderwissen über ein Unternehmen, eine Organisation oder ein Unternehmen, die ein potenzielles Risiko darstellen könnten, indem sie Sicherheitsrichtlinien mit der Absicht verletzen, Schaden anzurichten.

Internet der Dinge (IoT) Bezieht sich auf die Fähigkeit von Alltagsgegenständen (anstelle von Computern und Geräten), eine Verbindung mit dem Internet herzustellen. Beispiele sind Wasserkocher, Kühlschränke und Fernseher.

Eindringen Ein nicht autorisierter Akt der Umgehung der Sicherheitsmechanismen eines Netzwerks oder Informationssystems.

Intrusion Detection System (IDS) Programm oder Gerät, das verwendet wird, um zu erkennen, dass ein Angreifer unbefugten Zugriff auf Computerressourcen hat oder versucht, diesen zu erlangen.

Intrusion Prevention System (IPS) Intrusion Detection System, das auch den unbefugten Zugriff blockiert, wenn er erkannt wird.

Keylogger Software oder Hardware, die Tastenanschläge und Tastaturereignisse verfolgt, in der Regel heimlich, um Aktionen des Benutzers eines Informationssystems zu überwachen.

Malvertising Verwendung von Online-Werbung als Liefermethode für Malware.

Malware (bösartige Software) ein Begriff, der Malware, Trojaner, Würmer oder jeglichen Code oder Inhalte enthält, die negative Auswirkungen auf Organisationen oder Einzelpersonen haben könnten. Software zur Infiltrierung und Beschädigung oder Deaktivierung von Computern.

Entschärfung Die Anwendung einer oder mehrerer Maßnahmen zur Verringerung der Wahrscheinlichkeit eines unerwünschten Ereignisses und/oder zur Minderung seiner Folgen.

Netzwerk Zwei oder mehr Computer, die miteinander verbunden sind, um Ressourcen gemeinsam zu nutzen.

(Externe) Outsider-Bedrohung Eine Person oder Gruppe von Personen außerhalb einer Organisation, die nicht berechtigt sind, auf ihre Vermögenswerte zuzugreifen und ein potenzielles Risiko für die Organisation und ihre Vermögenswerte darstellen.

Passwort Eine Zeichenfolge (Buchstaben, Zahlen und andere Symbole), die zum Authentifizieren einer Identität oder zur Überprüfung der Zugriffsberechtigung verwendet wird.

Passwort-Cracker Programme, die darauf ausgelegt sind, ein Passwort zu erraten, oft durch Durchlaufen häufig verwendeter Kombinationen oder unter Verwendung eines Benutzernamens und eines Passworts, das von einem Konto erhalten wurde, bei dem ein Verstoß aufgetreten ist.

Passwort-Manager Programme, mit denen Benutzer Passwörter an einem Ort sicher generieren, speichern und verwalten können.

Patching Anwenden von Updates auf Firmware oder Software zur Verbesserung der Sicherheit und/oder Verbesserung der Funktionalität.

Pentest (Durchdringungstests) Ein autorisierter Test eines Computernetzwerks oder -systems, der darauf ausgelegt ist, nach Sicherheitslücken zu suchen, damit diese behoben werden können.

Personenbezogene Daten (PII) Die Informationen, die es ermöglichen, die Identität einer Person direkt oder indirekt abzuleiten.

Pharming Ein Angriff auf die Netzwerkinfrastruktur, der dazu führt, dass ein Benutzer auf eine illegitime Website umgeleitet wird, obwohl der Benutzer die richtige Adresse eingegeben hat.

Phishing Ungezielte Massen-E-Mails, die an viele Menschen gesendet werden und nach sensiblen Informationen (wie Bankdaten) fragen oder sie ermutigen, eine gefälschte Website zu besuchen. Eine digitale Form des Social Engineering, um den Einzelnen zu der Bereitstellung sensibler Informationen zu verleiten.

Klartext Unverschlüsselte Informationen.

Proxyserver Server, der als Vermittler zwischen Benutzern und anderen Servern fungiert und Benutzeranforderungen validiert.

Ransomware Schädliche Software, die Daten oder Systeme unbrauchbar macht, bis das Opfer eine Zahlung macht.

Wiederherstellung Die Aktivitäten nach einem Zwischenfall oder Ereignis zur kurz- und mittelfristigen Wiederherstellung wesentlicher Dienste und Operationen und zur vollständigen Wiederherstellung aller Funktionen auf längere Sicht.

Resilienz Die Fähigkeit, sich an sich ändernde Bedingungen anzupassen und sich auf Störungen vorzubereiten, zu widerstehen und sich schnell von Störungen zu erholen.

Wiederherstellung Die Wiederherstellung von Daten nach Computerausfall oder -verlust

Risikobewertung Der Prozess des Identifizierens, Analysierens und Bewertens von Risiken zusammen mit den potenziell schädlichen Folgen zum Zweck der Information über Prioritäten, der Entwicklung oder des Vergleichs von Handlungsoptionen und der Information der Entscheidungsfindung.

Sicherheitsinformations- und Ereignismanagement (SIEM) Prozess, bei dem Netzwerkinformationen aggregiert, sortiert und korreliert werden, um verdächtige Aktivitäten zu erkennen.

Smishing Phishing per SMS: Massen-SMS, die an Benutzer gesendet werden und in denen um vertrauliche Informationen (z. B. Bankdaten) gebeten oder zum Besuch einer gefälschten Website aufgefordert wird.

Signatur Ein erkennbares, differenzierendes Muster. Zu den Arten von Signaturen gehören: Angriffssignatur, digitale Signatur, elektronische Signatur.

Social Engineering Manipuliert Personen bei der Durchführung bestimmter Aktionen oder der Weitergabe von Informationen, die einem Angreifer von Nutzen sind.

Software Bezieht sich auf Programme zum Betrieb eines Computers oder zur Verarbeitung elektronischer Daten.

Spam Der Missbrauch elektronischer Messaging-Systeme, um wahllos unerwünschte Massennachrichten zu senden.

Spear-Phishing Eine gezieltere Form von Phishing, bei der die E-Mail so gestaltet ist, als ob sie von einer Person stammt, die der Empfänger kennt und/oder der sie vertraut.

Spoofing Fälschung der Absenderadresse einer Übertragung, um illegalen [unbefugten] Zugang zu einem sicheren System zu erlangen. Imitieren, Maskieren, Piggybacking und Nachahmen sind Formen des Spoofings.

Spyware Malware, die Informationen über die Aktivitäten eines Computerbenutzers an eine externe Partei weitergibt.

Lieferkette Ein System von Organisationen, Personen, Aktivitäten, Informationen und Ressourcen zum Erstellen und Verschieben von Produkten, einschließlich Produktkomponenten und/oder Dienstleistungen von Lieferanten bis zu ihren Kunden.

System Im Allgemeinen bezieht sich auf ein System von einem oder mehreren Computern oder Geräten, die Daten und Informationen eingeben, ausgeben, verarbeiten und speichern.

Systemadministrator (Admin) Person, die Serverkonfigurationen (Hardware und Software) installiert, konfiguriert, behebt und verwaltet, um ihre Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten; verwaltet auch Konten, Firewalls und Patches; verantwortlich für Zugriffskontrolle, Passwörter, Kontoerstellung und -verwaltung.

Bedrohung Etwas, das einem System oder einer Organisation schaden könnte.

Bedrohungsakteur Eine Person, Gruppe, Organisation oder Regierung, die schädliche Aktivitäten durchführt oder beabsichtigt.

Trojaner (Trojanisches Pferd) Ein Computerprogramm, das als legitime Software getarnt ist, aber mit einer versteckten Funktion, die verwendet wird, um in den Computer des Opfers zu hacken. Eine Art von Malware.

Zwei-Faktor-Authentifizierung (2FA) Die Verwendung von zwei verschiedenen Komponenten zum Überprüfen der beanspruchten Identität eines Benutzers. Wird auch als Multi-Faktor-Authentifizierung bezeichnet.

Virtuelles privates Netzwerk (VPN) Ein verschlüsseltes Netzwerk, das häufig erstellt wird, um sichere Verbindungen für Remotebenutzer zu ermöglichen, z. B. in einer Organisation mit Büros an mehreren Standorten.

Virus Ein Computerprogramm, das sich selbst replizieren, einen Computer ohne Erlaubnis oder Wissen des Benutzers infizieren und dann auf einen anderen Computer ausbreiten kann. Eine Art von Malware.

Sicherheitsanfälligkeit Eine Sicherheitsanfälligkeit oder ein Fehler in der Software, einem System oder Prozess. Ein Angreifer kann versuchen, eine Sicherheitsanfälligkeit auszunutzen, um unberechtigten Zugriff auf ein System zu erhalten.

Whaling Hochgradig gezielte Phishing-Angriffe (als legitime E-Mails maskiert), die sich an Führungskräfte richten.

Wurm Ein sich selbst replizierendes, sich selbst verbreitendes, in sich geschlossenes Programm, das Netzwerkmechanismen nutzt, um sich zu verbreiten. Eine Art von Malware.

Definitionen aus Ressourcen zusammengestellt, die erstellt wurden von:

British Standards Institute
https://www.bsigroup.com/en-GB/Cyber-Security/Glossary-of-cyber-security-terms/

National Cyber Security Centre (NCSC -UK)
https://www.ncsc.gov.uk/information/ncsc-glossary

National Initiative for Cybersecurity Careers and Studies (NICCS -US)
https://niccs.us-cert.gov/about-niccs/cybersecurity-glossary

Zusätzliche Ressourcen:

Glossar des Australian Cyber Security Centre

https://www.cyber.gov.au/acsc/view-all-content/glossary

Global Knowledge
https://www.globalknowledge.com/us-en/topics/cybersecurity/glossary-of-terms/

SANS Institute: Glossar der Sicherheitsbegriffe
https://www.sans.org/security-resources/glossary-of-terms/