Cyber-Absicherung für Firmenkunden

Wie Ihre Mitarbeiter Gefahren erkennen und abwehren

Auch die modernste Absicherung von Netzwerken und Endgeräten weist Sicherheitslücken auf, wenn die eigenen Mitarbeiter eine Handvoll Grundregeln nicht befolgen. Dabei sind gefährliche E-Mail-Anlagen einfach zu erkennen, sichere Passwörter schnell zu erstellen und betrügerisches Verhalten ist leicht abzuwehren.

Auf den folgenden Seiten unterstützen wir Sie dabei, Ihre Mitarbeiter durch wertvolle Tipps und Hilfestellungen zu sensibilisieren und die Voraussetzungen zu Ihrer Antragsfrage zu erfüllen.

Regelungen im Umgang mit Passwörtern

- Anforderungen an interne Passwörter
- Passwörter erstellen und merken – Satzbaulogik

Regelungen zur verantwortungsvollen Nutzung des Internets

- Gefahren im Netz
- Verdachtsfälle überprüfen
- Erkennen, wohin der Link führt – privates Surfen
- Umgang mit E-Mails
- Verdächtige E-Mails – Phishing
- Phishing
- Umgang mit Phishing-E-Mails

Regelungen im Umgang mit Passwörtern

Anforderungen an interne Passwörter

Passwörter nicht mehrfach verwenden

Hat man sich einmal an ein Passwort gewöhnt, ist es praktisch und bequem, dieses für mehrere Benutzerkonten gleichzeitig zu verwenden. Doch das ist keine gute Idee, denn damit macht man Cyber-Kriminellen das Leben einfacher als nötig.

Passwortanforderungen

Sichere Passwörter erstellen

Aus Sicherheitsgründen sollten sämtliche Passwörter für die Anmeldung im Netzwerk, an Computern etc. folgenden Anforderungen entsprechen:

- Das Passwort muss mindestens 8 Zeichen lang sein.
- Das Passwort muss aus allen 4 Zeichentypen (Zahlen, Sonderzeichen, Klein- und Großbuchstaben) bestehen.
- Das Passwort muss spätestens alle 180 Tage gewechselt werden.

Ein Passwort sollte nicht aus Wörtern und Zahlen zusammengesetzt sein. Passwörter wie „MaxMeier1991!“ sind zu vermeiden. Generell sollten keine Geburtsdaten, Namen oder Kfz-Kennzeichen als Komponenten für Passwörter genutzt werden.

Mehrfachverwendung

Firmeninterne Passwörter dürfen nicht im Internet verwendet werden

Jedes Passwort darf ausschließlich für ein einziges Benutzerkonto verwendet werden. Wird es nach 180 Tagen ersetzt, ist es nicht erlaubt, das Passwort dann für ein anderes Konto zu nutzen. Verwenden Sie niemals ein Passwort für mehr als ein Benutzerkonto gleichzeitig. Passwörter, die Sie für firmeninterne Anwendungen einsetzen, sollten Sie niemals privat nutzen. Dies gilt auch umgekehrt: Hatten Sie ein Passwort beispielsweise schon für Ihr privates E-Mail-Konto im Gebrauch, sollte es später nicht im Berufsleben zum Einsatz kommen.

Geheimhaltung

Passwörter müssen geheim gehalten werden

Genau wie die PIN-Nummer der Bankkarte sind Passwörter vertraulich zu behandeln. Der beste Aufbewahrungsort für Passwörter ist das Gehirn. Alternativ können die Passwörter verschlüsselt aufgeschrieben oder ebenfalls verschlüsselt in einem Passwort-Safe gespeichert werden.

Beachten Sie

Passwörter sollten vor Ablauf der 180 Tage immer dann geändert werden, wenn:

- jemand Ihr Passwort erfahren haben könnte,
- ein Kollege, der bei Ihnen im Zimmer saß, die Firma verlässt,
- der Verdacht besteht, dass sich ein Trojaner auf dem Gerät (PC, Smartphone, Tablet etc.) befindet, von dem aus Sie sich eingeloggt haben.

<– zurück zur Übersicht

Regelungen im Umgang mit Passwörtern

Passwörter erstellen und merken – Satzbaulogik

Komplexe Passwörter

Erstellen und ganz einfach merken

Passwörter werden immer länger und komplexer. Sie bestehen aus kleinen sowie großen Buchstaben, Zahlen und Sonderzeichen.

Ein Beispiel: **„1MsiWgsus.“**

Es scheint unmöglich, sich ein solches Passwort einfach zu merken. Dabei ist es eigentlich ganz simpel.

Tipp

Denken Sie einfach in Sätzen und Bildern

Das genannte Beispiel basiert auf einem Kinderlied:

„**E**in **M**ännlein **s**teht **i**m **W**alde **g**anz **s**till **u**nd **s**tumm.“
„1MsiWgsus.“

Es setzt sich aus den Anführungszeichen und den ersten Buchstaben der Wörter zusammen und ergibt somit eine komplexe Abfolge aus zwölf Zeichen.

Das Passwort beginnt und endet mit Anführungszeichen. Das nächste Wort ist „Ein“, also eigentlich eine Zahl, dafür schreiben Sie die „1“. Für „Männlein“ das große „M“ und das kleine „s“ für „steht“ usw. und schon haben Sie ein sicheres und komplexes Passwort, das einfach zu merken ist. Denn Sie merken sich nicht das Passwort als kryptische Zeichenreihenfolge, sondern nur den Satz.

(Nehmen Sie nicht das hier verwendete Beispiel – benutzen Sie einen Satz aus Ihrem Leben, der zu Ihnen passt und Sie beispielsweise an ein positives Erlebnis erinnert.)

Ein zusätzlicher Trick …

… wäre übrigens, das Wort „und“ durch das kaufmännische „&“-Zeichen zu ersetzen. Das macht das Passwort noch sicherer:

„1MsiWgs&s.“

Wichtig: Nicht aufgeben! Es kann sein, dass Sie ein, zwei Wochen üben müssen, bevor diese Gedächtnistechnik funktioniert.

<– zurück zur Übersicht

Gefahren im Netz

Grundregeln beachten

Heutzutage sind das Internet und seine vielfältigen Möglichkeiten aus dem unternehmerischen Umfeld nicht mehr wegzudenken. Allerdings lauern beim Surfen im Netz jede Menge Gefahren. Aus diesem Grund sollten folgende Grundregeln unbedingt beachtet werden:

- Löschen Sie in regelmäßigen Abständen den Browser-Verlauf. Auch Cookies sollten von Zeit zu Zeit gelöscht werden.
- Nutzen Sie beim Download von Dateien aus dem Internet nur bekannte, renommierte Quellen.
- Vermeiden Sie es, persönliche und beruflich relevante Informationen im Netz preiszugeben.
- Nutzen Sie, soweit möglich, nur SSL-verschlüsselte Seiten bei der Recherche im Internet. Diese erkennen Sie am Kürzel „https“ vor der URL in der Adresszeile oder an einem Schloss-Symbol neben der URL.

Grundregeln Downloads

Das Herunterladen von Daten aus dem Internet lässt sich im heutigen Arbeitsalltag selten ganz umgehen. Schnell landen neben harmlosen Dokumenten auch Viren und Trojaner auf der Festplatte. Um Ihre eigene Sicherheit und die des Unternehmensnetzwerks nicht zu gefährden, sollten Sie beim Download aus dem Internet die folgenden Regeln einhalten.

Download erlaubt

Betrieblich notwendige Dateien

Erlaubt ist ausschließlich das Herunterladen betrieblich notwendiger Dateien. Downloads für den privaten Gebrauch sind generell untersagt.

Auf die Quelle achten

Woher kommt die Datei?

Überprüfen Sie genau, woher eine Datei stammt, bevor Sie sie herunterladen. Fragen Sie sich, ob die Quelle allgemein bekannt und als Anbieter von Downloads etabliert ist oder ob Sie eine Trojaner-Infektion riskieren. Sollten Sie sich unsicher sein, ob der Anbieter einer Datei vertrauenswürdig ist, hilft es oft, ihn zu googeln. Sollten andere Internetnutzer über Probleme mit den Downloads aus der betreffenden Quelle berichten, unterlassen Sie das Herunterladen.

Handelt es sich bei der Datei, die Sie herunterladen möchten, um ein Update oder eine Software, nutzen Sie zum Download wenn möglich die offizielle Website des Herstellers.

Download verboten

Rechtswidrige Inhalte

Der Download von eindeutig rechtswidrigen Dateien ist ausnahmslos untersagt. Dabei handelt es sich unter anderem um rechtsradikale, gewaltverherrlichende und pornografische Inhalte.

Das Herunterladen von Raubkopien urheberrechtlich geschützten Materials (z. B. Filme und Musik) ist ebenfalls verboten.

<– zurück zur Übersicht

Regelungen zur verantwortungsvollen Nutzung des Internets

Verdachtsfälle überprüfen

VirusTotal – Verdacht prüfen

Der kostenlose Dienst VirusTotal **(www.virustotal.com/de)** erlaubt es Ihnen, verdächtige Dateien und Webseitenadressen (URLs) auf jegliche Arten von Schadsoftware (Würmer, Viren, Trojaner etc.) überprüfen zu lassen.

Es sollte bei der Nutzung von VirusTotal darauf geachtet werden, dass keine vertraulichen oder sensiblen Daten hochgeladen werden, durch die man unter Umständen gegen Datenschutzgesetze verstößt.

Verdächtige Dateien prüfen

Auf Nummer sicher gehen

Verdächtige Dateien können Sie auf der Webseite von VirusTotal ganz einfach hochladen. Sie werden auf den Servern des Dienstes gespeichert und dort eingehend analysiert. Innerhalb weniger Sekunden wird Ihnen angezeigt, ob Schadsoftware erkannt werden konnte oder nicht.

Verdächtige URL prüfen

Präventiv handeln

Auch Webseitenadressen lassen sich überprüfen. Dafür kopieren Sie am besten den Link zur potenziell verdächtigen Webseite und geben ihn auf VirusTotal ein. Auch hier dauert der Prüfvorgang nur wenige Sekunden. Anschließend wird mitgeteilt, ob die Seite vertrauenswürdig ist oder ob Gefahren in Form von Schadsoftware drohen.

Grundregeln Hyperlinks

Hyperlinks können auf unterschiedliche Art zur Gefahr für Rechner und Netzwerke werden: Ein Klick kann beispielsweise den Download eines Trojaners starten, auf eine infizierte Webseite führen oder auf ein Webformular verweisen, in das man sensible Informationen eintragen soll.

Nicht einfach öffnen!

Die wichtigste Regel zuerst

Öffnen bzw. folgen Sie niemals Hyperlinks, die Sie nicht persönlich angefordert haben. Das gilt auch dann, wenn sie von einem vermeintlich vertrauenswürdigen Absender kommen. Rufen Sie diesen im Zweifelsfall an, um sicherzustellen, dass die E-Mail auch wirklich von ihm stammt.

Darüber hinaus müssen die im Folgenden aufgeführten Möglichkeiten der Überprüfung ausgeschöpft werden, bevor ein Link angeklickt wird.

Mouseover

Wohin führt der Link?

Nehmen Sie jeden Hyperlink genau unter die Lupe. Prüfen Sie mithilfe der Mouseover-Methode, ob der angezeigte Link auch wirklich auf die angegebene Webseite verweist. Fahren Sie mit dem Mauszeiger über den Link, ohne ihn anzuklicken. Nun öffnet sich ein Fenster, das die URL (= die Webadresse) der verlinkten Seite anzeigt. Kommt Ihnen die Webseite verdächtig vor, folgen Sie dem Link nicht.

<– zurück zur Übersicht

Erkennen, wohin der Link führt – privates Surfen

Ziel-URL erkennen

Kryptische Adressen entschlüsseln

URLs lassen sich sehr einfach verschleiern, indem man weitere Informationen vor oder hinter die eigentliche Adresse setzt. Um aus einer langen URL wie

http://www.sicherheit.online.hacker.to/test/login

das eigentliche Ziel herauszufiltern, gehen Sie folgendermaßen vor:

- Suchen Sie den ersten Slash (/) rechts nach „http://“.
- Gehen Sie von dort aus zurück nach links zum zweitnächsten Punkt.

Zwischen diesem Punkt und dem nächsten Slash steht die wahre Zieladresse, in diesem Fall „zieladresse.de“.

URL prüfen

Gefährlich oder nicht?

Prüfen Sie Hyperlinks über die Webseite **www.virustotal.com**. Hier können Sie die URL eingeben. Verschiedene Antivirenprogramme scannen die Zielseite anschließend und suchen nach versteckten Viren und Trojanern.

Privates Surfen am Arbeitsplatz

Sollte die private Nutzung des Internets erlaubt sein, sind folgende Punkte wichtig:

- Private Dateien dürfen nicht auf der Festplatte Ihres betrieblich genutzten PCs oder des betriebseigenen Servers gespeichert werden.
- Verwenden Sie keine privaten USB-Sticks oder andere Speichermedien an firmeneigenen Rechnern.
- Loggen Sie sich während der Arbeitszeit nicht in private Accounts (soziale Netzwerke, E-Mail, Online-Banking etc.) ein.
- Rufen Sie keine strafrechtlich bedenklichen Seiten auf (etwa mit pornografischen oder rechtsradikalen Inhalten).
- Privates Surfen im Internet ist während der Arbeitszeit erlaubt, darf Sie aber nicht von beruflichen Pflichten abhalten.

<– zurück zur Übersicht

Regelungen zur verantwortungsvollen Nutzung des Internets

Umgang mit E-Mails

E-Mails sind wie Postkarten

E-Mails haben ihren festen Platz unter den beliebtesten elektronischen Nachrichten der heutigen Zeit. Dabei wird gerne übersehen, dass sie nicht unbedingt zu den sichersten Kommunikationsmitteln gehören. Denn eine durchschnittliche E-Mail wird unverschlüsselt (spätestens beim Verlassen des Firmennetzwerkes) und somit im Klartext versendet.

Eine einigermaßen technisch versierte Person kann eine solche Nachricht einfach mitlesen. Daher haben E-Mails tatsächlich den Charakter einer Postkarte, die ohne Umschlag unterwegs ist. Denken Sie daran, wenn Sie eine „normale“ E-Mail verfassen.

Verschlüsselung

Datenschutz

Die Öffentlichkeit im Internet kann man in der Regel nicht sehen, sie ist aber dennoch vorhanden. Daher gilt: In unverschlüsselte E-Mails gehören keinerlei sensible Daten.

Vor allem personenbezogene Daten dürfen nicht ungeschützt übermittelt werden. Wer dies missachtet, muss ggf. mit rechtlichen Konsequenzen rechnen. Das Datenschutzgesetz schreibt vor, dass E-Mails mit entsprechendem Inhalt so verschickt werden müssen, dass sie nicht von Unbefugten gelesen, kopiert, verändert oder gelöscht werden können.

Alternativ

Anhang verschlüsseln

Haben Sie keine Möglichkeit, die E-Mail selbst zu verschlüsseln, sollten Sie sensible Informationen in Form eines verschlüsselten Anhangs versenden. PDFs lassen sich beispielsweise mit einem Kennwort schützen. Dieses Kennwort sollte natürlich nicht in der E-Mail stehen, sondern am besten telefonisch an den Empfänger übermittelt werden.

Umgang mit E-Mail-Anhängen

Viren und Trojaner gelangen heute am häufigsten über präparierte E-Mail-Anhänge auf Computer. Sie können Daten abgreifen, Prozesse manipulieren oder sabotieren und ganze Netzwerke lahmlegen. Beim Umgang mit Anhängen ist also höchste Vorsicht geboten.

Mit Bedacht vorgehen

Anhänge erst überprüfen

Prüfen Sie Ihre E-Mails in Ruhe. Achten Sie auf Plausibilität, beispielsweise auf Zusammenhänge mit aktuellen Arbeitsvorgängen. Passen z. B. Betreff und Inhalt nicht zusammen, gilt erhöhte Vorsicht. Öffnen Sie E-Mail-Anhänge nur, wenn Sie betrieblich notwendig sind. Stellen Sie zudem sicher, dass Ihnen der Absender bekannt ist.

Hinweis: Selbst wenn die E-Mail inklusive Anhang von einer Ihnen persönlich bekannten Person oder einem Kollegen kommt, kann sie einen Virus enthalten. Denn E-Mails können auch ohne Wissen des Absenders in dessen Namen verschickt werden, z. B. wenn dessen PC infiziert ist.

<– zurück zur Übersicht

Verdächtige E-Mails – Phishing

Herkunft klären

Ein kurzer Anruf hilft

Ist Ihnen der Absender einer E-Mail nicht bekannt, öffnen Sie den Anhang auf keinen Fall. Handelt es sich um einen potenziellen neuen Kunden oder Kooperationspartner, vergewissern Sie sich telefonisch, dass die Nachricht tatsächlich vom angegebenen Absender stammt.

Verdächtige Anhänge

Sofort melden!

Erhalten Sie eine E-Mail, deren Anhang verdächtig aussieht, etwa aufgrund einer doppelten Dateiendung wie „Dateiname.docx.exe“, melden Sie dies umgehend der IT-Abteilung. Öffnen Sie eine verdächtige Datei niemals selbst. Hinweis: Vorsicht auch bei verschlüsselten Anhängen. Diese werden besonders gerne als Transportmöglichkeit für Schadsoftware verwendet, da Antivirenprogramme sie nicht scannen können.

Was ist Phishing?

Angeln nach Daten

Der Begriff „Phishing“ ist ein Kunstwort und kommt vom englischen „fishing“ (angeln, fischen). Er beschreibt unter anderem den Versuch, über gefälschte E-Mails und Webseiten an die persönlichen Daten eines Internetnutzers zu gelangen, um damit Identitätsdiebstahl zu begehen. Cyber-Kriminelle versuchen also bildlich, nach Benutzerdaten und Passwörtern zu angeln und verwenden dafür verschiedene Köder.

Nach diesen Informationen wird besonders oft gefischt:

- Bankdaten
- Kreditkartendaten
- Geheimzahlen für Geldautomaten und Online-Banking
- Passwörter

Methoden

Täuschend echt

Typischerweise beginnt ein Phishing-Angriff mit einer E-Mail, die offiziell gehalten ist und den Empfänger oft sogar mit Namen anspricht. Als Absender wird beispielsweise ein bekanntes Kreditinstitut angegeben.

Die Nachricht verweist auf eine Webseite, die derjenigen des imitierten Unternehmens täuschend ähnlich sieht, oder enthält ein Formular. Hier wird der Nutzer unter einem Vorwand (etwa eine Aktualisierung der Kundendatenbank) zur Eingabe seiner (Zugangs-)Daten aufgefordert. So gelangen die Informationen in die Hände der Datendiebe.

Eine andere Methode des Phishings ist es, Schadsoftware auf dem Rechner des Nutzers zu installieren, etwa wenn dieser eine entsprechend präparierte Webseite besucht oder einen verseuchten Anhang öffnet.

Anschließend können beispielsweise alle Tastenanschläge des Opfers aufgezeichnet und sein gesamtes Internetverhalten kann überwacht werden.

<– zurück zur Übersicht

Phishing

Folgen von Phishing

Transaktionen in Ihrem Namen

Mit Ihren Daten kann ein Cyber-Krimineller erheblichen Schaden anrichten. Er könnte:

- Ihr persönliches Konto belasten (z. B. durch maßloses Online-Shopping) oder neue Konten eröffnen,
- Verträge (z. B. für Dienstleistungen oder Mietverträge) in Ihrem Namen abschließen,
- Verbrechen unter Angabe Ihrer persönlichen Daten begehen (beispielsweise in Ihrem Namen Daten stehlen),
- in sozialen Netzwerken Imageschäden verursachen, was insbesondere für Unternehmen sehr heikel ist.

Eine erfolgreiche Phishing-Attacke kann also katastrophale Folgen haben.

Gefahren bei eingehenden E-Mails erkennen

Dass mit einer E-Mail auch gleichzeitig die eine oder andere Gefahr im Posteingang landet, ist bekannt. Doch wie können Sie diese enttarnen? Die folgenden Tipps geben Ihnen Anhaltspunkte, wie Sie die am häufigsten vorkommenden Risiken erkennen können.

Manipulierte Anhänge

Der Klassiker

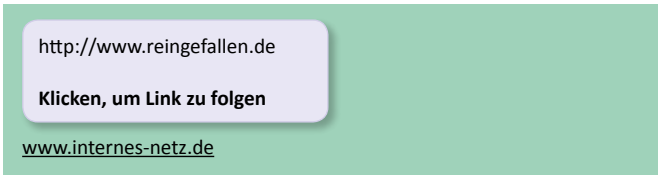
Sie haben eine E-Mail mit Anhang erhalten und wissen nicht, ob darin Schadsoftware schlummert? Dann haben Sie nun folgende Möglichkeiten, eine Gefährdung vor dem Öffnen des Anhangs zu entdecken:

- Kam der Anhang unerwartet bzw. unaufgefordert und ist der Absender unbekannt, sollten Sie ihn nicht einfach öffnen.
- Achten Sie auch bei bekannten Absendern auf einen passenden Kontextbezug, d. h., überlegen Sie, ob das Anliegen zum Absender und Ihren Aufgaben passt.
- Prüfen Sie den Anhang, beispielsweise auf: **www.virustotal.com**

Hyperlinks

Nicht täuschen lassen

Auch hinter einem Link kann sich eine Falle verbergen. Nutzen Sie hier zunächst das sogenannte „Mouseover“. Zeigen – nicht klicken – Sie also mit dem Cursor auf den Link, dann wird der Mouseover-Dialog eingeblendet. Ist der hinterlegte Link der gleiche wie der, den Sie als Text sehen?



Überlegen Sie zudem, ob die Webseite, auf die verlinkt wird, Ihnen bekannt ist und seriös erscheint. Im Zweifel lieber nicht auf den Link klicken.

Genauso wie Dateien können Sie auch Hyperlinks auf **www.virustotal.com** prüfen.

<– zurück zur Übersicht

Regelungen zur verantwortungsvollen Nutzung des Internets

Umgang mit Phishing-E-Mails

Phishing

Indizien

Bei gut gefälschten Phishing-E-Mails können Sie bestenfalls anhand von Indizien feststellen, ob es sich um eine solche handelt. Offensichtliche Merkmale treten nur noch selten auf – früher konnte man die bösartigen Nachrichten an einer kryptischen Absenderadresse, einer falschen oder unvollständigen Ansprache oder unzähligen Rechtschreibfehlern erkennen. Hilfreich ist aber wiederum der Versuch, die erhaltene E-Mail in einen sinnvollen Kontext zu bringen.

Allgemeingültig

Vorsicht ist besser als Nachsicht

Generell gilt: Ein gesundes Misstrauen ist durchaus angebracht. Ungewöhnliche Aufforderungen oder Anfragen per E-Mail sollten Sie immer hinterfragen. Sind Sie sich unsicher, dann investieren Sie lieber noch eine Minute für einen kurzen Anruf beim vermeintlichen Absender, als einen falschen Klick zu riskieren.

Gefahren durch aktive Inhalte in Office-Dokumenten

Aktive Inhalte, auch Makros genannt, sind kleine Programme, die in Dokument-Dateien eingebettet sind. In Microsoft Word z. B. können damit bestimmte Prozesse automatisiert werden und dem Benutzer die Arbeit erleichtern. Makros können aber auch so programmiert werden, dass sie wie herkömmliche Viren und Trojaner funktionieren und als schädlich einzustufen sind. Cyber-Kriminelle setzen Makroviren beispielsweise ein, um Dateien auf einem befallenen Computer zu kopieren, zu löschen oder zu verschlüsseln. Aktuelle Antivirenprogramme erkennen viele, aber leider nicht alle Gefahren, die von aktiven Inhalten in Office-Dokumenten ausgehen.

Auf diese Weise manipulierte bzw. instrumentalisierte Office-Dokumente werden häufig per E-Mail-Anhang versendet.

Makros deaktivieren

Risiken minimieren

Um Ihren PC vor den Gefahren in Makros zu schützen, sollten Sie diese deaktivieren. Das geht folgendermaßen:

- Öffnen Sie das Office-Programm, für das Sie die Makros deaktivieren wollen.
- Klicken Sie auf die Registerkarte „Datei“ und anschließend auf „Optionen“.
- Klicken Sie auf „Trust Center“ und dann auf „Einstellungen für das Trust Center“.
- Klicken Sie hier auf „Makroeinstellungen“.
- Nun können Sie die gewünschten Einstellungen vornehmen. Empfehlenswert ist die Auswahl der Option „Alle Makros ohne Benachrichtigung deaktivieren“. So werden aktive Inhalte und damit auch Makroviren nicht mehr automatisch nach dem Öffnen einer Datei ausgeführt.

Hinweis: Die Änderungen gelten jeweils nur für das Office-Programm, über das Sie die betreffenden Einstellungen vornehmen.

Das Merkblatt wurde in Zusammenarbeit mit unserem Kooperationspartner 8com erstellt.

Mit dem Abschluss des Cyber-Bausteins können Sie das Awareness-Portal unseres Kooperationspartners 8com sechs Monate kostenlos nutzen und Ihre Mitarbeiter schulen und informieren – mit zahlreichen weiterführenden Unterlagen. Ihre Zugangsunterlagen zum Awareness-Portal erhalten Sie nach Abschluss des Cyber-Bausteins.

Nähere Informationen zu den Cyber-Versicherungen von AXA finden Sie unter:
https://www.axa.de/geschaeftskunden/cyber-versicherung

AXA Versicherung AG, 51171 Köln
axa.de