WHITE PAPER

SECURITY AWARENESS LIBRARY

KOMPETENT CYBER CRIME KONTERN

Cyber Crime boomt. Dieser bestürzende Fakt ist jedem klar, der Wirtschaftspresse und Fachmedien verfolgt. Experten überschlagen sich geradezu mit immer neuen Warnungen, Schadensmeldungen und Fallzahlen. Dennoch verlassen sich in zu vielen Unternehmen und Behörden noch immer zu viele Menschen allein auf die Technik. Und damit sind sie Cyber Gangstern ausgeliefert, die immer neue Wege finden, um die Firewall zu überwinden. Corona und die Vereinzelung im Home Office haben diesen Trend noch verstärkt. Dazu gesellt sich menschliches Fehlverhalten - der Mensch ist die größte Sicherheitslücke. Zugleich sind gerade Kolleginnen und Kollegen mit Misstrauen und Achtsamkeit die besten Wachtposten von sensiblen Daten. Und sie sind auch die letzte Verteidigungslinie gegen IT-Kriminelle. Daher müssen die Sinne der Belegschaft permanent geschärft werden. Genau hier setzt die neue Security Awareness Library an: Das Portal setzt mit interaktiven Video-Modulen auf einen nachhaltigen Lerneffekt der User. Wir erläutern in diesem White Paper die Hintergründe in Sachen Cyber Crime. Und erklären die Funktionsweise der Security Awareness Library.

EXECUTIVE SUMMARY

DAS IST DIE SECURITY AWARENESS LIBRARY (SAL)

- Die Security Awareness Library ist ein Kompendium von Trainingsfilmen in Sachen Cyber Crime, Informations- und Datensicherheit. Auf einer eigenen Website finden sich zum Start zehn E-Learnings zu dringenden Themen in Sachen Security Awareness.

- Die E-Bibliothek schärft die Sinne der User, trainiert Misstrauen und Achtsamkeit. Sie resultiert aus dem Joint Venture der mybreev GmbH und der Deutsche Telekom Security GmbH, konkret: dem Team Security Awareness.

- Wir sensibilisieren gegen die Gefahren von Cyber Crime und eigener Unachtsamkeit: Ein zu schneller Click auf Anhänge von Phishing-Mails und die Malware frisst sich durch das IT-System. Zu laute Telefonate und ein Industriespion hört mit. Versäumte IT-Updates – schon dringt ein neuer Trojaner ein. Ein unordentlicher Schreibtisch und die Konkurrenz freut sich über sensible Informationen. Dokumente, die auf Dienstreise offen auf dem Bett liegen und ein ausländischer Geheimdienst schlägt zu.

- Wir trainieren mit der Library alle Angehörigen einer Organisation auf Management- wie Arbeitsebene unabhängig ihrer Fachrichtung in Sachen Security Awareness.

- Aufbau und Anmutung sind modern und im Netflix-Stil gehalten. User klicken sich durch interaktive Videos, die mit Grafik, Quiz und Text-Einblendungen aufgelockert sind.

- Die E-Bibliothek wird auch in der Deutschen Telekom für das Training genutzt. Sie ist ein Beispiel für Produkte, mit denen das Team Security Awareness auch auf dem kommerziellen Markt seit geraumer Zeit aktiv ist.

- Wir gehen davon aus, dass die Nachfrage nach schnell verfügbaren, überall einsetzbaren Lerntools in Zukunft rasant anzieht. Denn Cyber Crime hat sich inzwischen weltweit zu einem für Kriminelle lukrativen Geschäftsmodell entwickelt.

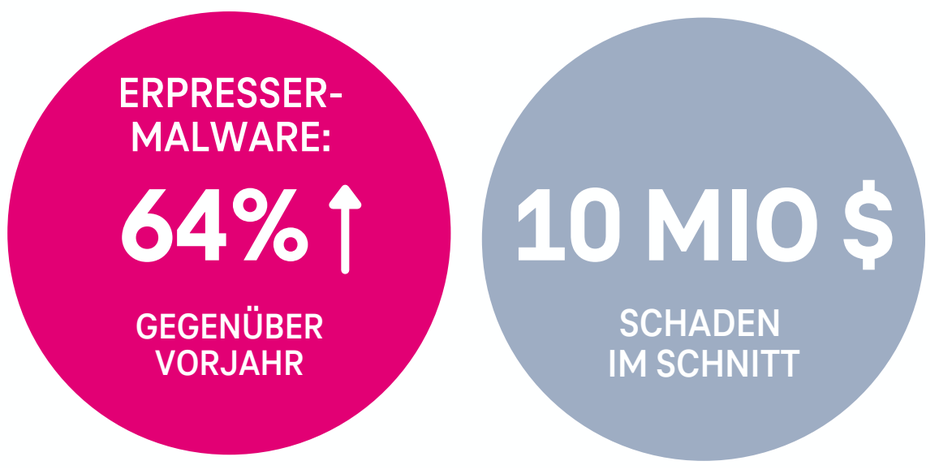
WARUM: CYBER CRIME BOOMT

Die Security Awareness Library reagiert auf eine erschreckende Zunahme in der Web-Kriminalität. Cyber Crime hat sich in den vergangenen Jahren zu einer florierenden globalen Branche entwickelt. Malware, Phishing, Chefbetrug, Klau von vertraulichen Dokumenten, IT-Sicherheitslücken. Dazu gesellt sich Social Engineering, also das Vortäuschen einer anderen Identität. Trojaner, DDoS-Geschwader und vor allem Erpresser-Programme kosten Staaten, Behörden, Krankenhäuser, Universitäten oder Firmen Milliarden.

Kein Land ist sicher. Allein in Deutschland liegt der Gesamtschaden bei rund 220 Milliarden Euro. (1) Ein neuer Rekord, urteilt der Branchenverband Bitkom. Neun von zehn Unternehmen werden von Mitte 2020 bis 2021 Opfer eines Angriffs. (2)

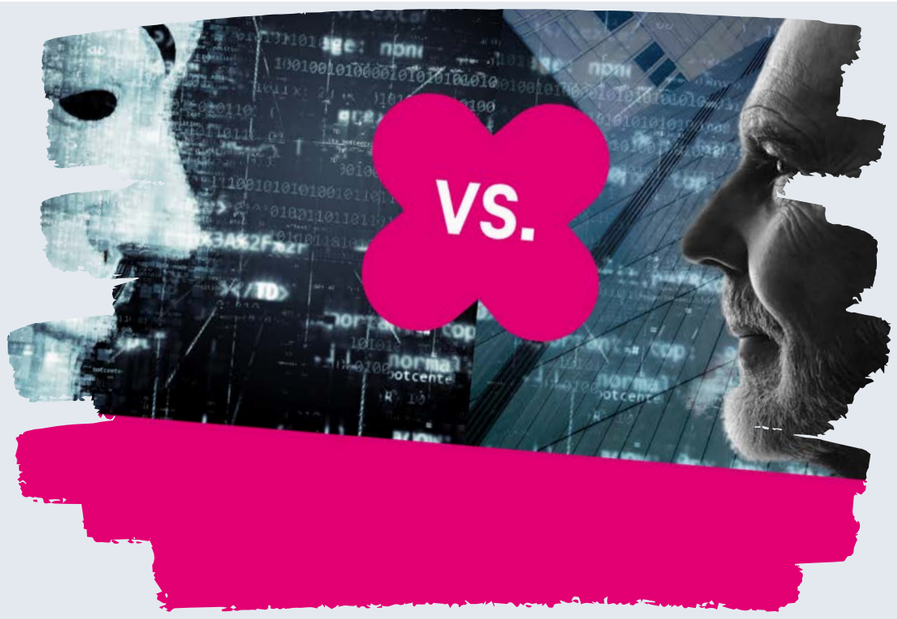
Besonders en vogue ist zuletzt das Einschleusen von Erpresser-Malware gewesen: Im August 2021 meldete die IT-Security-Firma Barracuda Networks einen bedeutenden weltweiten Anstieg der großen Ransomware-Angriffe. Insgesamt untersuchte sie in den vergangenen zwölf Monaten 121 Erpresser-Attacken – ein Plus von 64 Prozent gegenüber dem Vorjahr. Die Durchschnittliche Lösegeld-Forderung beträgt demnach 10 Millionen Dollar. (3), (4)
Interpol warnt derweil vor einer kommenden Ransomware-Pandemie. (5) Und die gerade erkannte Log4j-Sicherheitslücke erhöht das Sicherheitsrisiko.

Das Geschäft ist lukrativ und das Risiko gering: Die Angreifer können schnell und unerkannt im Darkweb abtauchen, sie sind im Ausland vor dem Zugriff von Ermittlern des FBI oder BKA sicher. Und Konzerne, deren Websites und IT-Systeme wochenlang lahmgelegt werden, sind häufig bereit, zu zahlen.



WARUM: CYBER WAR

Die Banden sind professionell, geduldig und diszipliniert. Experten sprechen von Advanced Persistent Threats oder APT – anhaltende Bedrohungen auf hohem Niveau. Und sie warnen vor einem Cyber War. Die Kriminellen spionieren ihre Opfer mitunter monatelang aus, bevor sie zuschlagen. Ein spektakuläres Beispiel für diese neue Form der Bedrohung ist die Invasion des Microsoft Exchange Server Anfang 2021. Zehntausende Firmen und Organisationen werden danach infiltriert. (6) - (8)



Das Opfer Microsoft macht eine bislang unbekannt chinesische Gruppe für die Massen-Kompromittierung verantwortlich. Der Software-Konzern nennt die Hacker Hafnium. (9) - (15)

Zuvor läuft 2020 der wohl größte Spionage-Fall aller Zeiten. Tausende von Unternehmen installieren ein Update für die Software Solarwinds Orion. Doch damit laden viele den eingeschleusten Trojaner Sunburst hoch. Dieser verbindet sich mit dem Command-and-Control-Server der Angreifer. Die Befehle: Daten auslesen, Netzwerk analysieren, weitere Schadcodes laden. Selbst das Pentagon, das US-Finanz- und Handelsministerium sowie das Europa-Parlament tappen in die Falle. Hinter dem Angriff auf Solarwinds steht westlichen Fahndern zufolge die Gruppe Cozy Bear. Für NSA, FBI und die US-Cybersicherheitsbehörde CISA steht fest: Auftraggeber ist der russische Auslandsgeheimdienst. Die USA verhängen Sanktionen gegen Russland. (16) - (21)

Im Frühjahr 2021 fordert das russische Hacker-Kollektiv REvil/Sodinokibi rund 50 Millionen Dollar von Acer. Ob und wieviel der taiwanesische Computer-Hersteller gezahlt hat, ist unklar. Im Juni 2021 gibt der brasilianische Fleischkonzern JSB eine Lösegeld-Zahlung von 11 Millionen Dollar in Bitcoin an die gleiche Gruppe zu. Kurz danach startet REvil eine Ransomware-Attacke auf die amerikanische IT-Firma Kaseya. 1.500 Kunden werden von Schadsoftware befallen. REvil verlangt 70 Millionen Dollar Lösegeld in der Crypto-Währung Bitcoin – die bis dato höchste bekannte Forderung aller Zeiten. (22), (23)

www.security-island.com/sal

Endlich schaltet sich das Weiße Haus ein. Im Juli 2021 fordert US-Präsident Joe Biden von Russlands Präsident Wladimir Putin ein härteres Vorgehen gegen Cyber-Kriminelle. (24)

Und dann die große Überraschung: REvil ist auf einmal spurlos verschwunden. Die Kontakt-Websites der Gruppe im Darknet und ihr Happy Blog sind abgeschaltet. Zwischendurch taucht sie wieder auf, doch Berichte über Festnahmen kursieren. Ob die Gruppe damit endgültig abgeschaltet wurde, ist unklar. (25)

Schon einmal hatte sich solch eine Hoffnung zerschlagen. 2014 hackt eine nordkoreanische Bande den Filmkonzern Sony Pictures Entertainment und richtet einen Schaden von 35 Millionen Dollar an. Zu dieser Zeit ist die Gang noch bekannt als Guardians of Peace. Dann verschwindet sie. Die totgeglaubte Gruppe formiert sich aber neu und ersteht quasi wieder auf. Sie wird fortan in der Branche Lazarus genannt. Im Februar 2016 stiehlt die Lazarus-Gang umgerechnet 80 Millionen Dollar von der Bangladesh Bank. (26), (27)

Im Mai 2017 schließlich die spektakuläre WannaCry-Attacke. Weltweit infiziert eine Erpressersoftware rund 300.000 Computer. Im Februar 2021 erhebt das US-Justizministerium Anklage gegen drei Mitglieder des nordkoreanischen Militärgeheimdienstes. (28), (29)

WARUM:

CORONA – DOPING FÜR HACKER

Die Corona-Pandemie hat die Flut der Bugs, Viren und Trojaner noch verstärkt. Denn beim Arbeiten im Home Office warten neue Herausforderungen – und für viele werden die eigenen vier Wände auch in Zukunft verstärkt das Büro ersetzen. Viele surfen zuhause mehr privat, ohne den robusten Firewall des Betriebes. Die Ablenkungen nehmen zu: Die Kinder wollen spielen, der Postbote klingelt. Mitunter ist der heimische Schreibtisch nicht ganz so aufgeräumt, wie in der Firma. Daher sehen neugierige Gäste vielleicht zu viel. Und wenn plötzlich eine verdächtige E-Mail einschlägt, können die Menschen anders als im Büro niemanden um Rat fragen.

Kriminelle nutzen diese neue Lage schamlos aus. Die Studie Cost of a Data Breach konstatiert im August 2021 mit 4,2 Millionen Dollar den höchsten durchschnittlichen Schaden in der 17jährigen Geschichte des Berichts. Das Ponemon-Institut und IBM Security hatten dazu 537 Verstöße untersucht. Zwei interessante Details der Untersuchung: Die meisten Angriffe wurden durch gestohlene Anmeldeinformationen verbucht - 20 Prozent der untersuchten Sicherheitsverletzungen gingen darauf zurück. Und die höchsten Kosten wurden durch kompromittierte geschäftliche E-Mails verursacht. (30), (31)

www.security-island.com/sal

WARUM:

DER FAKTOR MENSCH IN DER ABWEHR

Das Einfallstor für viele solcher Attacken sind Phishing-Kampagnen. In vielen Firmen überwinden die Hacker allzu oft Virenschutz und Firewall. Denn die IT-Kriminellen werden immer professioneller, da auch die Gegenwehr nachzieht und immer ausgefeilter wird. In einer gefakten Mail lässt sich mitunter ein Trojaner im Anhang oder in einem verseuchten Link einschleusen, ohne dass der Virenschutz dies bemerkt. Auch die Abwehr der Deutschen Telekom registriert diesen Trend: Gegen unseren Konzern beispielsweise laufen nach internen Informationen rund 60 Prozent aller Angriffe über Phishing.

Besonders schwer zu greifen für die Technik sind sogenannte Deepfakes, die am Telefon und per Video durchgezogen werden: Mit Hilfe von Künstlicher Intelligenz wandelt Software die Stimme jedes Angreifers in die gewünschte Tonlage eines Chefs oder Zulieferers um. Inzwischen ist diese Technologie schon für kleines Geld verfügbar. Hier hilft nur Misstrauen: Nachfragen, Interna gegenchecken und vor jeder geforderten Überweisung eine zusätzliche Autorisierung einholen. Mitdenken also.

Dass der Mensch als Einfallstor immer wichtiger wird, belegt auch ein perfider Fakt, den die IT-Security-Firma Intel 471 im Dark Web entdeckt hat: Demnach sind inzwischen in diversen Untergrund-Foren Stellenanzeigen aufgetaucht, in denen Hacker Englisch-Muttersprachler als geschickte Manipulatoren für BEC-Attacken suchen. Dieser Business E-Mail Compromise ist die Kompromittierung und Ausplünderung von Opfern, indem der Angreifer vortäuscht, ein Geschäftspartner zu sein – und per Mail eine Rechnung stellt. (32), (33)

WACHSAMKEIT UND WISSEN

CYBER GANGSTER STOPPEN

Wenn die technischen Sicherheitsbarrieren überwunden sind, macht unsere Wachsamkeit also den Unterschied aus zwischen dem Ausweichen vor einer Attacke und dem Daten-Gau. Am Ende steht der Mensch als letzter Schutzwall zwischen dem Geschäftserfolg und einem kritischen Hacker-Angriff. Doch nur wer weiß, wie Hacker, Diebe, Social Engineerer vorgehen und wie Selbstschutz funktioniert, wird professionelle Cyber-Banden, verärgerte ehemalige Mitarbeiter und Mitarbeiterinnen oder die allzu neugierige Konkurrenz abwehren.

Wer misstrauisch ist, denkt nach bei einer verdächtigen Mail. Checkt E-Mail-Adressen. Führt regelmäßige IT-Updates durch. Hinterfragt, ob eine angebliche Zahlungsanweisung tatsächlich von einem Zulieferer kommt. Hakt nach, ob wirklich der Chef oder eine Top-Managerin eine Zahlung in Auftrag gibt oder fragt sich, ob es tatsächlich eine neue Kollegin ist, die so viele Interna wissen möchte. Passt auf Dienstreisen auf und lässt keine sensiblen Dokumente ungeschützt im Hotelzimmer liegen. Und bemerkt logische Brüche und Schreibfehler in Phishing-E-Mails.

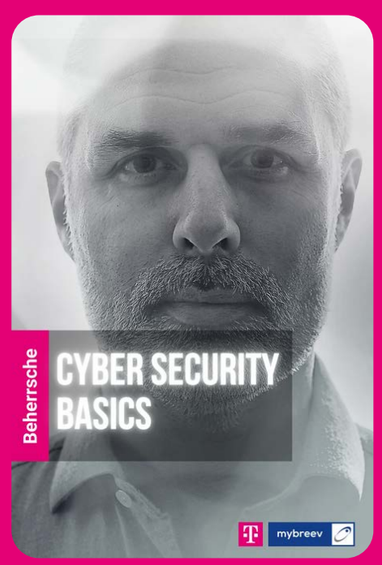
Wer all dies nicht leistet, riskiert das Ende der eigenen Karriere. Oder gar den Ruin der Firma.

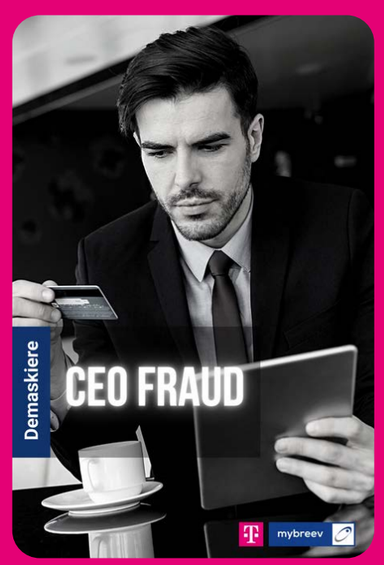
www.security-island.com/sal

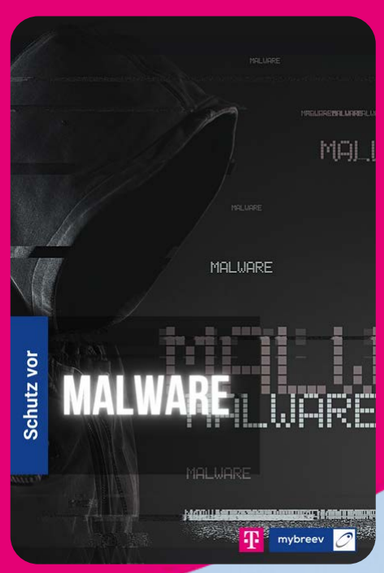
Unser
E-LEARNING-PORTFOLIO

Die Security Awareness Library sorgt für diese im Geschäftserfolg überlebensnotwendige Abwehrbereitschaft. Lernen mit einem professionellen Portfolio – hier finden Sie alles, was Sie brauchen, um im Kampf gegen IT-Kriminelle zu bestehen. Die interaktiven Schulungsfilme schärfen durch permanentes Training das Bewusstsein der User. Die Video-Module erzählen eine spannende Geschichte und fesseln daher die Leserinnen und Leser.

10 E-LEARNING-KURSE







Partizipierend

Sicherheit selbst in die Hand nehmen - mithilfe von realistischen Fallbeispielen und Quizelementen partizipieren alle Entscheider, Manager und Beschäftigten am E-Learning-Kurs. So wird jedes Thema greifbar gemacht!

Nachhaltig lernen

Die E-Learning-Kurse sind lernpsychologisch auf nachhaltiges Lernen ausgerichtet. Durch die relativ kurzen Lerneinheiten lassen sich Inhalte besser merken und im Unternehmensalltag leichter abrufen.

Individualisierbar

Benötigen Sie zusätzlich die Abbildung eines spezifischen Prozesses oder andere individuelle Inhalte? Wir individualisieren den Kurs sowohl inhaltlich als auch gestalterisch nach Ihren Vorgaben.

Leichter Zugang

Nutzen Sie unsere Kurse in Ihrem bestehenden LMS oder rufen Sie die Kurse in der mybreev Online Academy ab. On Premise oder in der Cloud schulen Sie unkompliziert Ihre Beschäftigten und behalten den Lernerfolg auf dem Dashboard stets im Auge.

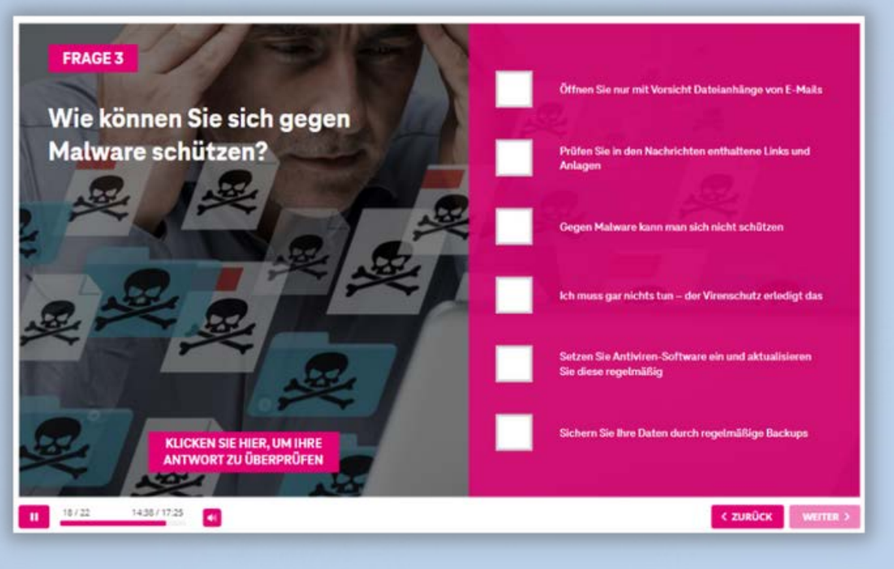
www.security-island.com/sal

Unser
E-LEARNING-PORTFOLIO

Die E-Learnings liefern zum einen aus der Praxis abgeleitete Beispiele. Zum anderen nehmen sie aber auch Fälle aus der Realität auf, die es in die Schlagzeilen geschafft haben.

Alle Lernenden können zudem Fachbegriffe oder Namen in den Sprechertexten nachlesen, falls sie die gesprochenen Worte nicht einordnen können.

Die Filme halten die Aufmerksamkeit der Zuschauer hoch, indem sie zwischen Video-Sequenzen, Zeichnungen, Grafiken und eingeblendeten Slogans hin und her wechseln – Text und Ton ergänzen sich.

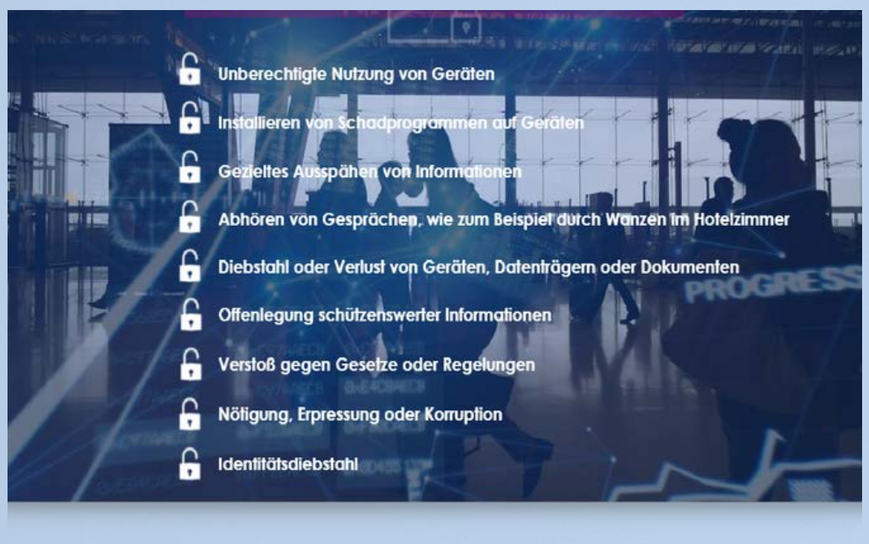


Die Länge der Module beträgt jeweils rund 15 bis 28 Minuten.

Das vermittelte Wissen wird durch einen Quiz nochmals verankert, um eine höhere Nachhaltigkeit zu erzeugen. Wer in die Module eintaucht, wird nicht nur einseitig belehrt – hier ist die Mitarbeit gefragt.

In einigen Modulen wartet eine Zusammenfassung als PDF.

Zu guter Letzt steht ein virtuelles Zertifikat.



Die Filme lassen sich als einzelne Trainingsvideos in Awareness-Kampagnen einbauen.

SPANNENDE CASES

NACHHALTIG

TAKE AWAYS

ZERTIFIKAT

www.security-island.com/sal

WIE: SO FUNKTIONIERT DIE SAL

Mit der Library nehmen Kolleginnen und Kollegen Daten- und Informationsschutz kompetent selbst in die Hand. Die Bedienung ist einfach und intuitiv, das Design modern und ansprechend. Unsere Kunden buchen unseren Service und erhalten einen Login für die Website. Interne User der Deutschen Telekom sind automatisch freigeschaltet. Der Zugang erfolgt über ein Intranet-Portal.

Die E-Bibliothek richtet sich nicht an die Fachleute aus der IT-Abteilung. Die Library adressiert stattdessen als Zielgruppe genau die Generalisten, die bevorzugt in die Schusslinie der IT-Kriminellen geraten: Sekretariat, Buchhaltung, Rechnungswesen, Management, Azubis.

Ein Vorteil der digitalen Lernbibliothek ist die Diskretion: Viele Menschen trauen sich nicht, vor ihren Chefs und den anderen im Büro Lücken zu offenbaren. Hier schafft das Lernen am Computer Abhilfe: Die User können sich Stellen, die sie nicht verstanden haben, noch einmal anschauen. Beliebig oft.

So ist das Lernen auf eine Gesellschaft zugeschnitten, die sich neben dem Fernsehen verstärkt über Video-Portale wie Netflix oder Magenta TV und über die Social Media informiert. Wer will, schaut sich die E-Learnings zum passenden Zeitpunkt an. Ganz nebenbei in der Mittagspause. Oder zwischen zwei Meetings.

Die digitale, schnell verfügbare Schulung hat somit für Kundinnen und Kunden einen weiteren Vorteil: Sie müssen nicht umständlich ein großes Meeting einberufen. Und sie sparen sich teure externe Trainer oder Unternehmensberater.

Unser Angebot hat auch die Fachwelt überzeugt. Die Security Awareness Library hat direkt zum Start einen renommierten Comenius Award gewonnen. Im Juli 2021 hat die Gesellschaft für Pädagogik, Information und Medien e.V. der Bibliothek ein Comenius EduMedia Siegel in der Kategorie Schulbildung und Erwachsenenbildung verliehen. Der renommierte Preis honoriert herausragende Leistungen in Sachen Didaktik.

www.security-island.com/sal

WER: ZWEI STARKE PARTNER

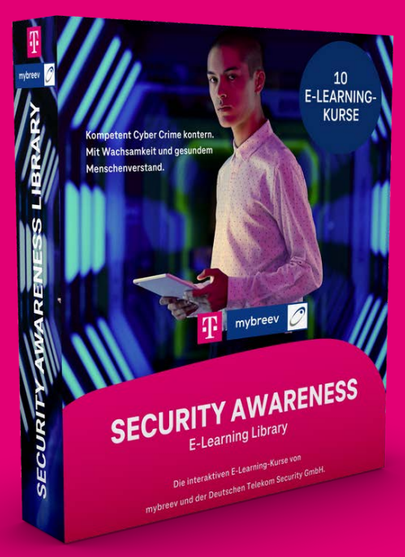
Mit mybreev und der Telekom Security GmbH haben sich zwei starke Partner zusammengeschlossen, die sich ideal ergänzen. Jeder bringt seinen eigenen Stil ein und seine Erfahrungen. Das gemeinsame Angebot ist die Security Awareness Library.

mybreev ist seit 2009 im Markt unterwegs und weiß, was Firmen brauchen.

2017 wurde in der T-Systems die Unit Telekom Security gegründet, die im Sommer 2020 in eine eigene GmbH ausgelagert wurde. Sie schützt auch die Deutsche Telekom weltweit. Kernstück der Abwehr ist das 2017 eröffnete integrierte Cyber Defense & Security Operation Center (SOC) in Bonn, das aktuell das größte seiner Art in Europa ist.

Die Erkenntnisse über Hacker-Attacken und weitere Sicherheitsgefahren werden in der Telekom Threat Library gespeichert, die mittlerweile gut 20 Millionen Einträge über Viren, Malware, APT-Attacken und Zero-Day Exploits und andere Sicherheits-Ereignisse enthält und damit eine der größten Datenbanken weltweit ist. Kurz: Wir wissen, wie wir die Banden stoppen.

Davon profitiert auch das Team der Security Awareness - die SAW ist führend in Sensibilisierung und Training in Sachen Sicherheit. Wir bringen den Menschen spielerisch und interaktiv aktuelles Wissen bei. Die Devise lautet: Die SAW belehrt nicht mit erhobenem Zeigefinger. Sondern führt jeden durch eigenes Nachdenken auf den richtigen Weg. Zu den Angeboten zählen beispielsweise das Kinderbuch AwareNessi, das ShowHacking oder der Security Parcours.



Sie benötigen eine moderne und zuverlässige Schulungslösung?

Kontaktieren Sie uns - gerne stellen wir Ihnen einen kostenlosen Demozugang zur Verfügung und unterstützen Sie bei der Implementierung.

Deutsche Telekom
Telefon: +49 (228) 181-0
E-Mail: Security-Awareness@telekom.de

mybreev
Telefon: +49 (2162) 106 554 9
E-Mail: office@mybreev.com

www.security-island.com/sal

QUELLENVERZEICHNIS (1|2)

(1) Quelle: heise.de. 03.09.2021 https://www.heise.de/news/)220-Milliarden-Euro-Schaden-durch-Ransomware-und-andere-Cyber-Angriffe-6156111.html?wt_mc=rss.red.security.security.atom.beitrag.beitrag

(2) Quelle: Lanline.de. 03.09.2021 https://www.lanline.de/it-security/cyberangriffe-betreffen-nahezu-neun-von-zehn-unternehmen.253361.htm

(3) Quelle: heise.de. 03.09.2021 https://www.heise.de/news/Ransomware-Attacken-nehmen-dramatisch-zu-6169583.html?wt_mc=rss.red.security.security.atom.beitrag.beitrag

(4) Quelle: Barracuda.com. 03.09.2021 https://blog.barracuda.com/2021/08/12/threat-spotlight-ransomware-trends/

(5) Quelle: zdnet.de. 03.09.2021 https://www.zdnet.de/88395786/ransomware-interpol-warnt-vor-exponentiellen-wachstum/?utm_source=feedly&utm_medium=rss&utm_campaign=rss

(6) Quelle: spiegel.de. 03.09.2021 https://www.spiegel.de/netzwelt/netzpolitik/usa-und-eu-werfen-china-hacker-angriffe-vor-a-794862ee-9ecb-444d-8b6b-ff56cccf80dd#ref=rss

(7) Quelle: us-cert.cisa.gov. 03.09.2021 https://us-cert.cisa.gov/ncas/current-activity/2021/07/19/us-government-releases-indictment-and-several-advisories-detailing

(8) Quelle: sueddeutsche.de. 03.09.2021 https://www.sueddeutsche.de/politik/usa-china-cyberattacke-ms-exchange-hacker-1.5356325

(9) Quelle: the register.com 03.09.2021 https://www.theregister.com/2021/07/19/hafnium_china_state_security/

(10) Quelle: dw.com 03.09.2021 https://www.dw.com/de/vom-angriff-auf-microsofts-exchange-server-k%C3%B6nnten-auch-viele-deutsche-unternehmen-betroffen-sein/a-56802966

(11) Quelle: krebsonsecurity.com 03.09.2021 https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software/

(12) Quelle: blogs.microsoft.com 03.09.2021 https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/

(13) Quelle: en.wikipedia.org 03.09.2021 https://en.wikipedia.org/wiki/Hafnium_(group)

(14) Quelle: blogs.microsoft.com 03.09.2021 https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/

(15) Quelle: edition.cnn.com 03.09.2021 https://edition.cnn.com/2021/03/03/tech/microsoft-exchange-server-hafnium-china-intl-hnk/index.html

(16) Quelle: spektrum.de 03.09.2021 https://www.spektrum.de/news/solarwinds-ein-hackerangriff-der-um-die-welt-geht/1819187

(17) Quelle: silicon.de 03.09.2021 https://www.silicon.de/41683773/solarwinds-hack-usa-beschuldigen-offiziell-hacker-des-russischen-geheimdiensts

(18) Quelle: computerwoche.de 03.09.2021 https://www.computerwoche.de/a/die-gefaehrlichsten-hackergruppen,3551190?utm_source=Security&utm_medium=email&utm_campaign=newsletter&pm_cat%5B1%5D=productivity+software&pm_cat%5B2%5D=kreativ+software&pm_cat%5B3%5D=security+allgemein&pm_cat%5B4%5D=cyberkriminalit%C3%A4t&tap=ab81aa70e1c33c88706cfd4e551c4fd5

QUELLENVERZEICHNIS (2|2)

(19) Quelle: en.wikipedia.org 03.09.2021 https://en.wikipedia.org/wiki/Cozy_Bear

(20) Quelle: spiegel.de 03.09.2021 https://www.spiegel.de/netzwelt/netzpolitik/solarwinds-hack-der-spionagefall-des-jahres-a-0b728cc4-d375-4cb9-9450-3635ca8172a0

(21) Quelle: silicon.de 03.09.2021 https://www.silicon.de/41683773/solarwinds-hack-usa-beschuldigen-offiziell-hacker-des-russischen-geheimdiensts

(22) Quelle: crn.com 03.09.2021 https://www.crn.com/news/security/revil-demands-record-70m-in-kaseya-ransomware-attack

(23) Quelle: computerwoche.de 03.09.2021 https://www.computerwoche.de/a/die-gefaehrlichsten-hackergruppen,3551190?utm_source=Security&utm_medium=email&utm_campaign=newsletter&pm_cat%5B1%5D=productivity+software&pm_cat%5B2%5D=kreativ+software&pm_cat%5B3%5D=security+allgemein&pm_cat%5B4%5D=cyberkriminalit%C3%A4t&tap=ab81aa70e1c33c88706cfd4e551c4fd5

(24) Quelle: tagesschau.de 03.09.2021 https://www.tagesschau.de/ausland/amerika/biden-putin-hacker-101.html

(25) Quelle: Zeit.de, 15.11.2021 https://www.zeit.de/digital/internet/2021-11/europol-ransomwaregruppe-revil-festnahmen-fbi-loesegeld

(26) Quelle: cyberpolicy.com 03.09.2021 https://www.cyberpolicy.com/cybersecurity-education/who-is-lazarus-north-koreas-newest-cybercrime-collective

(27) Quelle: computerwoche.de 03.09.2021 https://www.computerwoche.de/a/die-gefaehrlichsten-hackergruppen,3551190?utm_source=Security&utm_medium=email&utm_campaign=newsletter&pm_cat%5B1%5D=productivity+software&pm_cat%5B2%5D=kreativ+software&pm_cat%5B3%5D=security+allgemein&pm_cat%5B4%5D=cyberkriminalit%C3%A4t&tap=ab81aa70e1c33c88706cfd4e551c4fd5

(28) Quelle: de.wikipedia.org 03.09.2021 https://de.wikipedia.org/wiki/WannaCry

(29) Quelle: en.wikipedia.org 03.09.2021 https://en.wikipedia.org/wiki/Lazarus_Group

(30) Quelle: ibm.com 03.09.2021 https://www.ibm.com/de-de/security/data-breach

(31) Quelle: security-insider.de 03.09.2021 https://www.security-insider.de/sicherheitsvorfaelle-kosten-richtig-viel-geld-a-1049583/

(32) Quelle: intel471.com 03.09.2021 https://intel471.com/blog/bec-cybercrime-underground

(33) Quelle: threatpost.com 03.09.2021 https://threatpost.com/bec-scammers-native-english-speakers/169092/