bitbone

SCHWACHSTELLE MENSCH – Cybersecurity ist mehr als der Einsatz von Sicherheitssoftware

SECURITY AWARENESS

Cybersecurity ist mehr als der Einsatz von Sicherheitssoftware

IT-Sicherheit in Unternehmen bedeutet heute mehr als der alleinige Einsatz von Security-Software. Die aktuelle Bedrohungslage hat sich deutlich verändert. Cyberkriminelle setzen bei ihren Attacken vor allem auf zwei wesentliche Merkmale: nicht gepatchte Systeme und Unwissenheit seitens der Anwender.

SCHWACHSTELLE MENSCH

In der Mehrzahl der Cybersicherheitsvorfälle wird der Schaden durch menschliche Fehler wie Unkenntnis und mangelndes Problembewusstsein verursacht. Das kann sich auf verschiedenen Ebenen abspielen: von der Verwendung unzureichender Passwörter, über sehr gut gemachte Phishingmails, bis hin zu Social Engineering – dem Versuch von Trickbetrügern, das Vertrauen anderer Personen zu erschleichen, um an Informationen zu gelangen oder den Anwender dazu zu bringen, eine gewünschte Aktion auszuführen.

Sicherheitsrichtlinien können aber nur dann greifen, wenn sie ausreichend beachtet werden. Um alle Sicherheitserfordernisse dauerhaft zu verinnerlichen, bedarf es eines ständigen Lernprozesses jedes einzelnen Mitarbeiters, der erst dann nachhaltig greift, wenn das Erlernte zur Routine wird. Alle Mitarbeiter eines Unternehmens, angefangen mit der studentischen Hilfskraft, über die Assistenz der Geschäftsleitung, bis hin zu den einzelnen Abteilungsleitern und der Führungsebene, sollten über ein gewisses Grundverständnis für Informationssicherheit verfügen.

Nur wenn jeder mitdenkt und in der Lage ist, Gefahren selbstständig einzuschätzen, können Unternehmen sich umfassend vor Cyberbedrohungen absichern. Denn selbst die beste Security-Software und die detailliertesten Sicherheitsrichtlinien können nie alle Sicherheitsaspekte, mit denen Mitarbeiter im täglichen Berufsleben konfrontiert werden, vollständig abdecken.

Über

80 %

aller Cybersicherheitsvorfälle entstehen durch menschliche Fehler[1]

61 %

der von Cybercrime betroffenen Unternehmen wurden von ehemaligen Mitarbeitern geschädigt[5]

30 %

der Mitarbeiter räumen ein, dass sie die Anmeldedaten ihrer Arbeitscomputer an Kollegen weitergeben[5]

50 %

der betroffenen Unternehmen geben binnen 6 Monaten nach einer Cyberattacke ihr Geschäft auf[4]

52 %

der Unternehmen sehen Mitarbeiter als größte Bedrohung der Cybersicherheit [2]

[1] Kaspersky Security Awareness Broschüre 2019, S. 1
[2] Kaspersky-Studie „The cost of a data breach", 2018
[3] Kaspersky „Sorting out a Digital Clutter", 2019
[4] Trivadis DOAG18: DevSecOps Benchmark
[5] Deloitte Cyber-Security Report 2017, Teil 2

DEUTSCHLAND, BIST DU SICHER?

87106

Fälle von Cyberkriminalität im „engeren Sinne“ wurden 2018 in Deutschland polizeilich erfasst.[1] Die Dunkelziffer dürfte weit höher liegen.

61,4 Mio €

Schaden entstand durch Cyberkriminalität in Deutschland im Jahr 2018[1]

88%

mehr tägliche bis wöchentliche Angriffe gab es in den letzten fünf Jahren[2]

[1] Bundeskriminalamt Cybercrime-Bundeslagebild 2018
[2] Deloitte Cyber-Security Report 2017, Teil 2

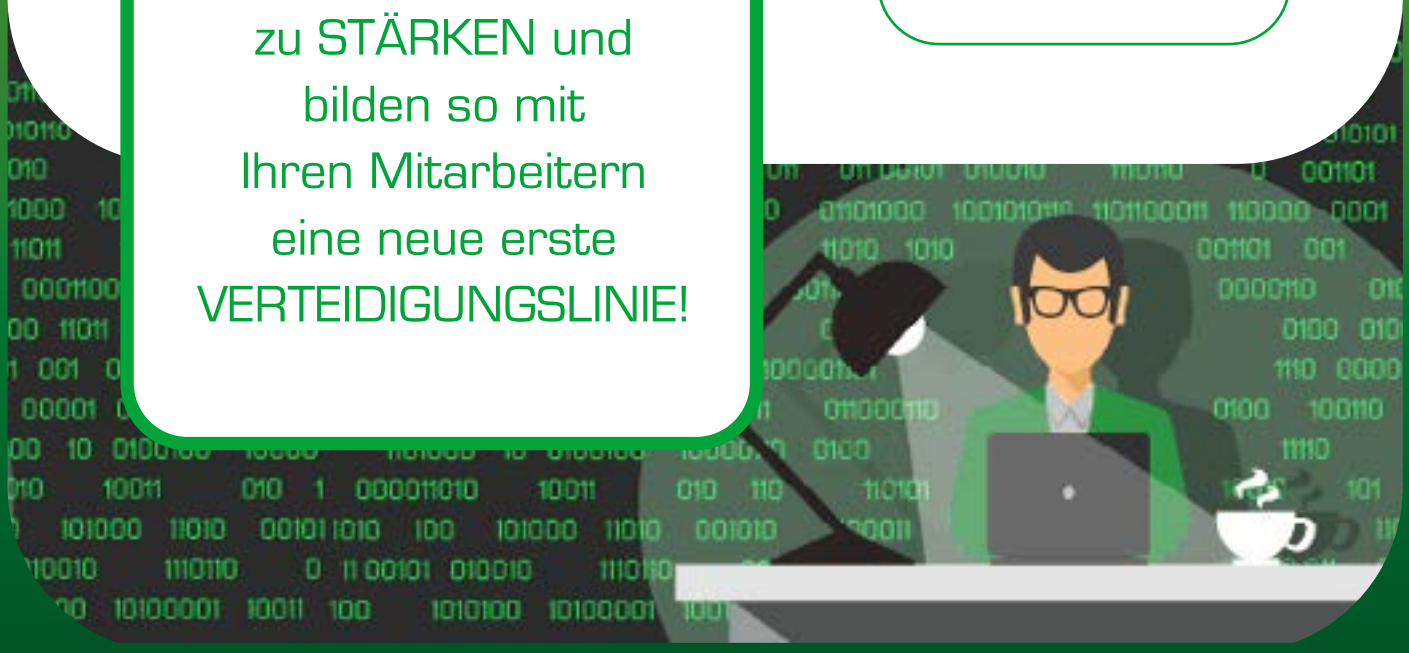
RISIKOBEWUSSTSEIN KORRELIERT MIT UNTERNEHMENSGRÖSSE

Führungskräfte großer Unternehmen zeigen im Durchschnitt ein deutlich höheres Bewusstsein für potenzielle Schäden durch Cybersecurity-Angriffe. Gleichzeitig steigt das Schadensbewusstsein von Mitarbeitern mit der Anzahl der erfolgten Angriffe.[2]
Die Auswirkungen durch Angriffe sind nicht nur finanzieller Art und lassen sich nur zum Teil direkt qualifizieren. Maßnahmen, die das Sicherheitsbewusstsein von Mitarbeitern stärken, sind ein effektiver Baustein innerhalb eines unternehmensweiten Risikomanagementkonzeptes.

Machen Sie durch SCHULUNGEN menschliche Schwächen zu STÄRKEN und bilden so mit Ihren Mitarbeitern eine neue erste VERTEIDIGUNGSLINIE!

33 %

der befragten Unternehmen beschäftigen sich nur anlassbezogen oder gar nicht mit Cybersecurity[2]



Security Awareness: Ein Bewusstsein für Cybersicherheit schaffen

Eine erhöhte Security Awareness seitens der User wird somit unabdingbar. Doch wie lässt sich diese sinnvoll erreichen? Gewöhnliche Cybersicherheitsschulungen haben deutliche Nachteile: Oftmals sind sie zu lang, zu technisch und uninteressant gestaltet, so dass sie Mitarbeiter nur schwer motivieren können. Damit die Schulungen eine lohnende Investition für Unternehmen darstellen, ist es von Bedeutung, dass Mitarbeiter direkt mit einbezogen werden.

Unser Partner Kaspersky Lab bietet ein mehrstufiges Online-Schulungsprogramm. Neben der Sicherheitsausbildung für IT-Mitarbeiter umfasst es Schulungen und Trainings, die alle Mitarbeiter in die Grundlagen der Cybersicherheit einweisen. Das breite Schulungsangebot verteilt sich auf unterschiedliche Sicherheitsaspekte und die entsprechenden Mitarbeiter. Für Unternehmen unterschiedlicher Größenordnung bedeutet die Vor-Ort-Schulung aller Mitarbeiter jedoch oftmals einen großen Zeit- und Arbeitsmehraufwand. Unterschiedliche Abteilungen und Mitarbeiter bedürfen individuellen Schulungsanforderungen. Wie lassen sich die verschiedenen Wissensstände und Bedürfnisse aller Mitarbeiter am besten vereinen, um das gemeinsame Ziel eines sicheren Unternehmens zu erreichen?

KASPERSKY AWARENESS SCHULUNGSFORMATE FÜR ALLE UNTERNEHMENSEBENEN

AWARENESS IN DER IT-ABTEILUNG: WARUM IST PATCH-MANAGEMENT SO WICHTIG?

Werden Systeme nicht rechtzeitig gepatcht, bieten Schwachstellen Angreifern eine leichte Möglichkeit, diese zu infiltrieren. Die Gründe für unzureichend gepatchte Systeme sind vielfältig und reichen von zu lang andauernden Patch-Prozessen bis hin zu IT-Abteilungen, die mit der großen Anzahl an unterschiedlichen Systemen schlichtweg überfordert sind. Aber auch zu kleine Budgets für IT-Security und Abhängigkeiten von Softwarelösungen, die auf den Systemen laufen und kein aktuelles Betriebssystem zulassen, zählen dazu.

Schlecht oder gar nicht installierte Aktualisierungen bieten Hackern einfache Angriffsziele. Dabei sind sowohl Betriebssysteme als auch Applikations-Software im Fokus der Cyberkriminellen. Planen, Testen und Installieren von Code-Änderungen an einer bestehenden Software zählen zu den Kerninhalten des Patch-Managements. Um solche Lücken umfassend und wirkungsvoll zu schließen, empfiehlt sich der Einsatz einer geeigneten Patch-Management-Lösung. Für moderne Enterprise Systemumgebungen bedarf es einer automatisierten Version, die auf Schwachstellen überprüft und gleichzeitig die Verfügbarkeit von Updates verwaltet. In Unternehmen eingesetzte Betriebssysteme und Anwendungssoftware werden dabei mit den Datenbanken des Patch-Management-Anbieters abgeglichen. Aktuelle Patches und Updates werden gemeldet und können dann automatisch oder individuell durch den Systemadministrator in die Umgebung eingepflegt werden.

Der Bedrohung einen Schritt voraus sein

Um Unternehmen vor kommenden Cyber-Attacken abzusichern, wird ein mehrschichtiger Sicherheitsansatz immer bedeutender. Da Mitarbeiter in den Fokus der Cyberkriminellen geraten, müssen diese stärker in ein ganzheitliches Security-Konzept eingebunden werden und selbst mit dem nötigen Know-how im Kampf gegen Cyberkriminelle ausgestattet werden. Cybersicherheitstrainings, die eine bessere Aufklärung und das richtige Bewusstsein für Gefahren fördern, sollten daher im Mittelpunkt eines ganzheitlichen Sicherheitskonzepts stehen.

Um in der heutigen Zeit sinnvoll vor Cyberkriminellen abgesichert zu sein, ist es zudem notwendig, ihnen einen Schritt voraus zu sein. Ausreichend gepatchte Systeme sowie nachhaltig geschulte und auf Sicherheit sensibilisierte Mitarbeiter bieten kein Angriffsziel mehr. Auch in Zeiten eines geringen Budgets sollte daher nicht auf Schulungsmaßnahmen verzichtet werden.

Automated Security Awareness Platform (ASAP)

Heutige Unternehmen sind zwar bestrebt, Programme zum Sicherheitsbewusstsein umzusetzen, viele von ihnen sind aber mit dem Verfahren und den Ergebnissen nicht zufrieden. Besonders für kleine und mittlere Unternehmen, die in der Regel kaum Erfahrung und dedizierte Ressourcen dafür haben.

Kaspersky® Security Awareness

Die Automated Security Awareness Platform (kurz: ASAP) ist ein Online-Tool für Mitarbeiter zur Förderung umfassender und praktischer Kenntnisse zur Cybersicherheit im Laufe eines Jahres. Zur Implementierung und Verwaltung der Plattform sind keine spezifischen Ressourcen und Vorbereitungen erforderlich und sie bietet dem Unternehmen integrierte Hilfe bei allen Schritten auf dem Weg hin zu einer sicheren Cyberumgebung im Unternehmen.

RISIKOSTUFEN FÜR VERSCHIEDENE ZIELGRUPPEN

Jedes Thema umfasst verschiedene Levels und bietet jeweils spezifische Kenntnisse im Bereich Sicherheit. Die Levels sind je nach dem Grad des Risikos definiert: Level 1 reicht in der Regel als Schutz vor einfachen und Massenangriffen aus. Zum Schutz vor komplexen und zielgerichteten Angriffen müssen die nächsten Levels abgearbeitet werden. Je höher das Risiko, desto höher sollte die Zielebene für die Schulung sein. Die Mitarbeiter der Personalabteilung und der Buchhaltung stellen typischerweise ein höheres Risiko als die meisten anderen dar.

SCHULUNGSTHEMEN

ASAP umfasst insgesamt 32 LERNMODULE mit je 10–20 Minuten Bearbeitungszeit zu folgenden Themen (u. a.):

- E- Mail
- Surfen im Internet
- Passwörter
- Soziale Netzwerke und Messenger
- PC-Sicherheit
- Mobile Geräte
- Vertrauliche Daten
- Persönliche Daten / DSGVO
- Social Engineering
- Sicherheit zu Hause und unterwegs

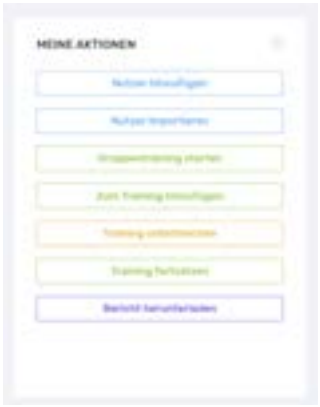
BEWUSSTSEINSMANAGEMENT FÜR UNTERNEHMEN JEDER GRÖSSE

- Schulungsziele festlegen
- Wissen vermitteln & festigen
- Fortschritt überwachen
- Mitarbeiter motivieren

ASAP PUNKTET

Bis zu **90 %**	Bis zu **50 %**	Bis zu **93 %**	Mehr als **86 %**	Mehr als **30x**
Reduzierung der IT-Sicherheits-vorfälle	Reduzierung der Kosten von IT-Sicherheits-vorfällen	Erfolgsquote, dass das Wissen im Alltag angewen-det wird	der Teilnehmer empfehlen Security Aware-ness Trainings weiter	ROI des Invest-ments in Security Awareness

DARUM ASAP



- ✓ Einfache Einrichtung, Verwaltung & Steuerung
- ✓ Kontinuierliches Lernen in einzelnen Schritten bei individuellem Lerntempo für jeden Mitarbeiter
- ✓ Mikrolearning-Inhalte im Umfang von 2 bis 10 Minuten
- ✓ Interaktive Lektionen und Videos, Tests und simulierte Phishing-Angriffe
- ✓ Tests über das Gelernte vor dem Fortfahren
- ✓ Kein Zeitaufwand für Analysen und manuelle Anpassungen
- ✓ Automatisierte Regeln nach gewünschter Schulungsebene, abhängig vom jeweiligen Risiko, das ein Benutzer trägt
- ✓ Lernmaterial nur im wirklich benötigten Umfang
- ✓ Dashboards mit erforderlichen Informationen zur Einschätzung des Fortschritts
- ✓ Automatische Standardreports mit Tipps zur Verbesserung
- ✓ Benchmarks
- ✓ 35 Sprachen verfügbar
- ✓ Ideal für Kleinunternehmer oder Mittelstand
- ✓ Zahlung nur für aktive Benutzer
- ✓ Für Reseller im MSP-Modell möglich

Kaspersky Interactive Protection Simulation (KIPS)

Kaspersky Interactive Protection Simulation (KIPS) ist ein Übungsszenario, bei dem IT-Sicherheitsteams aus Unternehmen und Behörden in eine simulierte Geschäftsumgebung versetzt werden, in der sie einer Reihe unerwarteter Cyberbedrohungen ausgesetzt werden, während die Teams versuchen, den Gewinn zu maximieren und das Vertrauen der Kunden zu erhalten.

Die Idee besteht darin, durch Auswahl der besten verfügbaren vorausschauenden und reaktionsschnellen Kontrollmöglichkeiten eine Cyberverteidigungsstrategie zu entwickeln. Jede Reaktion der Teams auf die eintretenden Ereignisse verändert den Verlauf des Szenarios und damit den Gewinn bzw. den Verlust des Unternehmens. Der Realitätsgrad der Ereignsisse ist beabsichtigt, da alle Szenarien auf realen Ereignissen basieren.

BRANCHENBEZOGENE KIPS-SZENARIEN

In den einzelnen Szenarien wird den Teilnehmern die Rolle der Cybersicherheit vor dem Hintergrund von Geschäftskontinuität und Rentabilität vermittelt. Dabei liegt das Hauptaugenmerk auf neu entstehenden Herausforderungen und Bedrohungen sowie gängigen Fehlern von Unternehmen beim Aufbau der eigenen Cybersicherheitsstrategie. Zudem wird die Zusammenarbeit zwischen Business- und Sicherheistteams gestärkt, die einen soliden Betrieb und nachhaltigen Schutz vor Cyberbedrohungen fördert.

WELCHE SZENARIEN GIBT ES?

UNTERNEHMEN
Schutz des Unternehmens, etwa vor Ransomware, APTs und Fehlern in der Automatisierungssicherheit

BANK
Schutz von Finanzinstituten vor ausgefeilten APTs, die Geldautomaten, Verwaltungsserver und Geschäftssysteme angreifen

E-GOVERNMENT/REGIERUNGSBEHÖRDEN
Schutz öffentlicher Webserver vor Angriffen und Exploits

KRAFTWERK/WASSERWERK
Schutz industrieller Steuerungssysteme und wichtiger Infrastrukturen

TRANSPORTWESEN
Schutz von Passagieren und Fracht vor Heartbleed, Ransomware und APTs

ÖL- UND GASINDUSTRIE
Lernen Sie die Folgen zahlreicher Bedrohungen kennen – von Website Defacement über aktuelle Ransomware bis hin zu durchdachten APTs

DAS ERWARTET SIE BEI KIPS:

- Machen Sie sich auf fortschrittliche Bedrohungen gefasst und erfahren Sie, wie Kriminelle technisch vorgehen (Threat Intelligence) und welche Ziele sie verfolgen.
- Erfahren Sie, wie Sie Vorfallsreaktion und Vorfallsprävention kombinieren.
- Testen Sie, was passiert, wenn Sie Ihre Sicherheitskontrollen nicht optimal konfiguriert sind.
- Halten Sie Ausschau nach gleichzeitigen Warnsignalen von Sicherheit, IT und Business.

KIPS FÜR ALLE, LIVE ODER ALS ONLINE-VERSION

KIPS richtet sich an Führungskräfte, Experten für Business-Systeme sowie IT-Experten, um deren Sicherheitsbewusstsein hinsichtlich der eigenen Risiken und Sicherheitsprobleme beim Betrieb moderner Computersysteme zu fördern.

Ob live gespielt oder als Online-Version (in 10 Sprachen): Spielen lohnt sich!

KIPS ONLINE:

- Ideal für Unternehmen mit weltweiten Standorten
- Gleichzeitige Nutzung durch bis zu 300 Teams
- Die Teams können die Spielschnittstelle in jeweils unterschiedlichen Sprachen nutzen
- Die Sitzungen werden durch einen Schulungsleiter über WebEx betreut

DARUM KIPS

KIPS ist besonders effektiv, denn es...

- ✓ bietet einen modernen, leicht umsetzbaren Ansatz zur Sensibilisierung der Mitarbeiter.
- ✓ ist kurzweilig, spannend und unterhaltsam.
- ✓ fördert die Zusammenarbeit im Team und gegenseitiges Verständnis.
- ✓ baut durch Konkurrenz die Bereitschaft zur Initiative sowie analytische Kompetenzen auf.
- ✓ ermöglicht den Aufbau von Cybersicherheit und sicherem Verhalten und dessen Analyse durch Entdeckungen und Fehler in Form eines Spiels.

KIPS fördert auf spielerische Weise strategische Entscheidungen sowie Kenntnisse rund um Cybersecurity.

Cybersecurity für IT Online (CITO-Schulung)

Die meisten Unternehmen bieten zweischichtige Cybersecurity-Schulungen an: Expertenschulungen für IT-Sicherheitsteams und Schulungen zur Verbesserung des Sicherheitsbewusstseins für Nicht-IT-Mitarbeiter. Die CITO Plattform von Kaspersky bietet interaktives Training für IT-Generalisten, wie z. B. IT-Support oder Service Desk, bei denen Standard-Awareness-Programme nicht ausreichen, aber fundiertes technisches Sicherheitswissen nicht erforderlich ist.

Die Lösung vermittelt praktische Fähigkeiten, die für das Erkennen eines möglichen Angriffs bei einem vermeintlich gutartigen PC-Vorfall und für das Sammeln von Daten zur Übergabe an die IT-Sicherheitsabteilung unerlässlich sind. Kurz: Incident Response Skills.

SCHULUNGSAUFBAU UND -THEMEN

Jedes Modul besteht aus einem kurzen theoretischen Überblick, praktischen Tipps und zwischen 4 und 10 Übungen. Mit jeder dieser Übungen wird eine besondere Kompetenz erlernt und demonstriert, wie IT-Sicherheitstools und -Software bei der täglichen Arbeit genutzt werden sollten. Die Schulung ist so angelegt, dass sie auf ein ganzes Jahr verteilt wird. Als Lerntempo wird eine Übung pro Woche empfohlen. Jede Übung nimmt etwa 5–45 Minuten in Anspruch.

- Überprüfung der Existenz oder Abwesenheit des Vorfalls im Zusammenhang mit Malware
- Das Arbeiten mit Systemen und Sandboxing-Lösungen sowie das Entfernen unerwünschter Programme und Dateien
- Durchführung von Netflow-Datenverkehrs-, Zeitachsen- und Ereignisprotokollanalysen
- Analyse von Phishing-E-Mails
- Sichere Servereinrichtung und Verifizierung der Sicherheitseinstellungen von Enterprise-Servern
- Das Erkennen und Patchen von Schwachstellen

WARUM IST CITO SO EFFEKTIV?

Die Plattform setzt sich aus einer Mischung aus einem kurzen Theorieteil, hilfreichen Tipps und einer Reihe praktischer Übungen zu spezifischen Kompetenzen des alltäglichen Arbeitslebens zusammen. Mit wenig Zeitaufwand lernt der User über einen längeren Zeitraum hinweg, regelmäßig und damit nachhaltig. Für den Einsatz der Plattform benötigen Anwender nur einen Internetzugang und einen Browser.

SO HANDELN USER OFT

SO SOLLTEN USER HANDELN

Benutzer

IT-Support/Admins

IT-Sicherheit

bitbone AG
Prymstraße 3 I 97070 Würzburg
T: +49 931 250993-10
M: sales@bitbone.de

www.bitbone.de

IHR PERSÖNLICHER ANSPRECHPARTNER

Veit Starke
Cybersecurity Expert
Sales
T: +49 931 250993-159
M: starke@bitbone.de

Stand: 01/2020