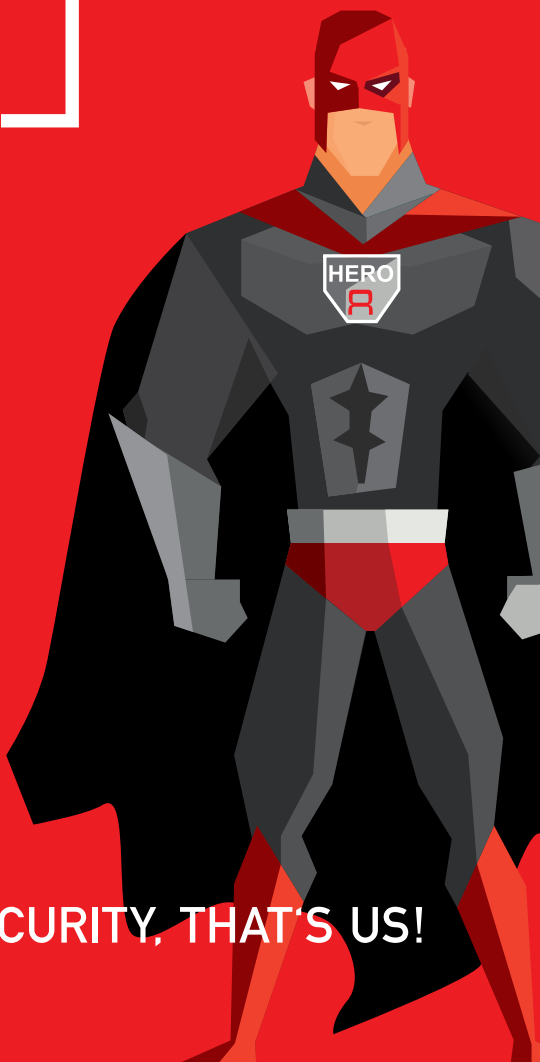
SECURITY SOFTWARE ALLEINE REICHT NICHT MEHR

SOFT

Experts Security Distribution



IT SECURITY, THAT'S US!

8SOFT GMBH

Mit mehr als 18 Jahren Expertise sind wir Ihr kompetenter und zuverlässiger Cybersecurity Distributor mit Herz.

Sie erhalten von uns ausschließlich exklusive Produkte namhafter Hersteller, die unseren Praxistest bestanden haben – aktuell sind dies: AppTec360, C-IAM, ESET, Fudo Security, Kaspersky und SEP Hybrid Backup.

Mit unseren Lösungen und Services möchten wir Ihnen weitere Wachstumschancen bieten, Sie in Ihrem täglichen Business unterstützen und dazu beitragen, Sie noch erfolgreicher zu machen.

Stellen Sie sich die Bausteine für Ihren Erfolg in unserem Partnerprogramm zusammen und profitieren von der Kraft der 8Soft-Gemeinschaft.

INHALT

WIE SIEHT DIE AKTUELLE BEDROHUNGSLAGE AUS?

87.106

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

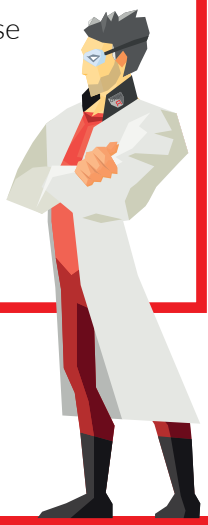
VORWORT

CYBERSECURITY IST MEHR ALS DER EINSATZ VON SECURITY SOFTWARE

IT-Sicherheit in Unternehmen bedeutet heute mehr als der alleinige Einsatz von Security Software. Die Bedrohungslage nimmt immer mehr zu, wie aktuelle Studien zeigen. Cyberkriminelle setzen bei ihren Attacken nicht mehr nur auf technische Sicherheitslücken wie ungepatchte Systeme, sondern zunehmend auf die Unwissenheit von Anwendern. Und, wie wir es aktuell erleben, nutzen sie gewissenlos selbst Pandemien bzw. die berechtigte Angst der Menschen davor für ihre Zwecke.

Die Agentur der Europäischen Union für Cybersicherheit (ENISA) beschreibt SECURITY AWARENESS als „das Bewusstsein für die Risiken und die verfügbaren Schutzmaßnahmen... und die erste Verteidigungslinie für die Sicherheit von Informationssystemen und -netzen". Jedes IT-SICHERHEITSKONZEPT muss demnach die „Komponente Mensch" viel stärker berücksichtigen als das bisher oft der Fall ist.

Für die Akzeptanz von Sicherheitsrichtlinien müssen Mitarbeiter diese allerdings als Schlüsselfaktoren für die Organisation betrachten, nicht als eine Reihe von Regeln, die ein effizientes Arbeiten einschränken.



60%

der gehackten kleinen und mittleren Unternehmen gehen nach sechs Monaten pleite.[3]

33%

der Organisationen, die Opfer einer Ransomattacke wurden, entschieden sich dafür, das geforderte Lösegeld zu zahlen.[4]

16 Tage

dauert es durchschnittlich in deutschen Unternehmen, bis ein kritisches Datenleck wieder geschlossen ist.[5]

[3] Trivadis DOAG18: DevSecOps Benchmark

[4] Proofpoint State-of-the-Phish-Bericht 2020

[5] https://www.servicenow.de/company/media/press-room/trotz-steigender-kosten-schlieben-von-lucken-bei-der-datensicherheit-dauert-immer-noch-wochen.html

SCHWACHSTELLE MENSCH

EIN UNNÖTIGES RISIKO

IN DER MEHRZAHL DER CYBERSICHERHEITSVORFÄLLE WIRD DER SCHADEN DURCH MENSCHLICHE FEHLER WIE UNKENNTNIS UND MANGELNDES PROBLEMBEWUSSTSEIN VERURSACHT.

80%

... aller Cybersicherheits-vorfälle entstehen durch menschliche Fehler.[1]

61%

... der von Cybercrime betroffenen Unternehmen wurden von ehemaligen Mitarbeitern geschädigt.[3]

52%

... der Unternehmen sehen Mitarbeiter als größte Bedrohung der Cyber-sicherheit.[2]

FACT & FIGURES

[1] Kaspersky Security Awareness Broschüre 2019, S. 1
[2] Kaspersky-Studie „The cost of a data breach", 2018
[3] Deloitte Cyber-Security Report 2017, Teil 2
[4] Proofpoint State-of-the-Phish-Bericht 2020
[5] https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-100-Milliarden-Euro-Schaden-pro-Jahr

Mangelndes Problembewusstsein, also mangelne Awareness, kann sich auf verschiedenen Ebenen abspielen: von der Verwendung unzureichender Passwörter, über sehr gut gemachte Phishing-Mails, 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. Gut geschulte Mitarbeiter sind ein sehr effektiver Schutz: zum Vorbeugen vor unbeabsichtigten Schäden, zur Abwehr von Angriffen von außen und zum rechtzeitigen Gegensteuern im Falle eines erfolgreichen Angriffs.

33%

... der deutschen Erwachsenen können den Begriff Phishing NICHT der korrekten Definition zuorden, bei Ransomware sind es 77%, Smishing 72%, und Vishing sogar 83%.[4]

102.900.000.000 €

SCHADEN

... entstand der deutschen Wirtschaft im Bemessungszeitraum 2018/2019 durch Sabotage, Datendiebstahl oder Spionage, analoge und digitale Angriffe zusammengenommen. Im Vorjahreszeitraum 2016/2017 waren es noch 55 Mrd. € p.a.

Die Anzahl digitaler Angriffe steigt; sie haben bei 70% der Unternehmen einen Schaden verursacht (2017: 43%).

Drei von zehn Angriffen werden rein zufällig entdeckt.[5]

UNSER TIPP:

Mitarbeiter ins Zentrum von Sicherheitskonzepten stellen und sie durch geeignete, nachhaltige Schulungs- & Aufklärungskampagnen dazu befähigen, eigenständig Angriffe zu erkennen und zu melden.

SECURITY AWARENESS

EIN BEWUSSTSEIN FÜR CYBERSICHERHEIT SCHAFFEN

EIN ERHÖHTES SICHERHEITSBEWUSSTSEIN DER USER IST EIN GROSSER SCHRITT ZUR MEHR SECURITY. 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.

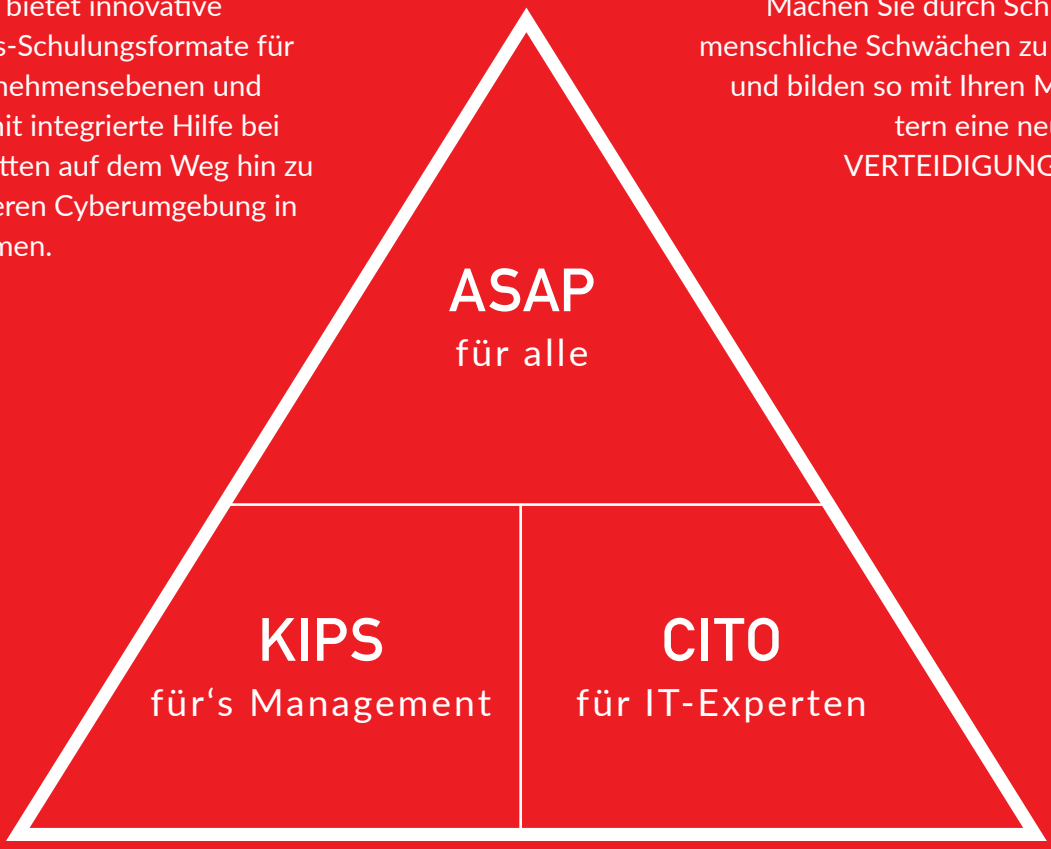
Für Unternehmen unterschiedlicher Größenordnung bedeutet die Vor-Ort-Schulung aller Mitarbeiter jedoch oftmals einen großen Zeit- und Arbeitsmehraufwand. Unterschiedliche Abteilungen und Mitarbeiter bedürfen individuellen Schulungsanforderungen. Wie lassen sich die verschiedenen Wissensstände und Bedürfnisse aller Mitarbeiter am besten vereinen, um das gemeinsame Ziel eines sicheren Unternehmens zu erreichen? Wir haben die Lösung: Kaspersky Awareness Trainings.

SCHULUNGSFORMATE

FÜR JEDE EBENE DAS PASSENDE FORMAT

Kaspersky bietet innovative Awareness-Schulungsformate für alle Unternehmensebenen und bietet damit integrierte Hilfe bei allen Schritten auf dem Weg hin zu einer sicheren Cyberumgebung in Unternehmen.

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



01

ASAP

Automated Security Awareness Platform

Sensibilisierung für die Cybersicherheit aller Mitarbeiter eines Unternehmens

02

KIPS

Kaspersky Interactive Protection Simulation

Planspiel für die Führungsebene zur Strategie- und Führungsunterstützung und mehr Verständnis für Cybersecurity-Maßnahmen

03

CITO

Cybersecurity for IT Online

Online-Plattform für IT-Experten zum Erlernen erster Gegenmaßnahmen bei Sicherheitsvorfällen in Unternehmen

AUTOMATED SECURITY AWARENESS PLATFORM

ASAP

AUFBAU & INHALT

32 Lernmodule mit je 10–20 Minuten Bearbeitungszeit bieten reichlich Know-how zu allen relevanten Bereichen (u. a.):

- E- Mail
- Surfen im Internet
- Passwörter & Konten
- Soziale Netzwerke & Messenger
- PC-Sicherheit
- Mobile Geräte
- Vertrauliche Daten
- Social Engineering
- Sicherheit zu Hause & unterwegs

Kaspersky® Security Awareness

ASAP IST EINE ONLINE-LERNPLATTFORM FÜR UNTERNEHMENSMITARBEITER ZUR FÖRDERUNG UMFASSENDER UND PRAKTISCHER KENNTNISSE ZUR CYBERSICHERHEIT.

Durch kurze aber regelmäßige Trainingseinheiten gelingt einerseits eine leichte Integration in den Arbeitsalltag, gleichzeitig wird ein nachhaltiger Lernerfolg erzielt.

Zur Implementierung und Verwaltung von ASAP sind keine spezifischen Ressourcen und Vorbereitungen erforderlich. Trainingsziele können individuell und abhängig vom potenziellen Risikolevel festgelegt und überwacht 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.

DAS RISIKOBEWUSSTSEIN KORRELIERT MIT DER UNTERNEHMENSGRÖSSE

Führungskräfte großer Unternehmen zeigen im Durchschnitt ein deutlich höheres Bewusstsein für potenzielle Schäden durch Cybersecurity-Angriffe. Gleichzeitig haben besonders kleine und mittlere Unternehmen kaum Erfahrung und dedizierte Ressourcen für Cybersecurity-Maßnahmen, also umso mehr Grund sich für ASAP zu entscheiden.

DARUM ASAP

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

SICHERER DANK ASAP

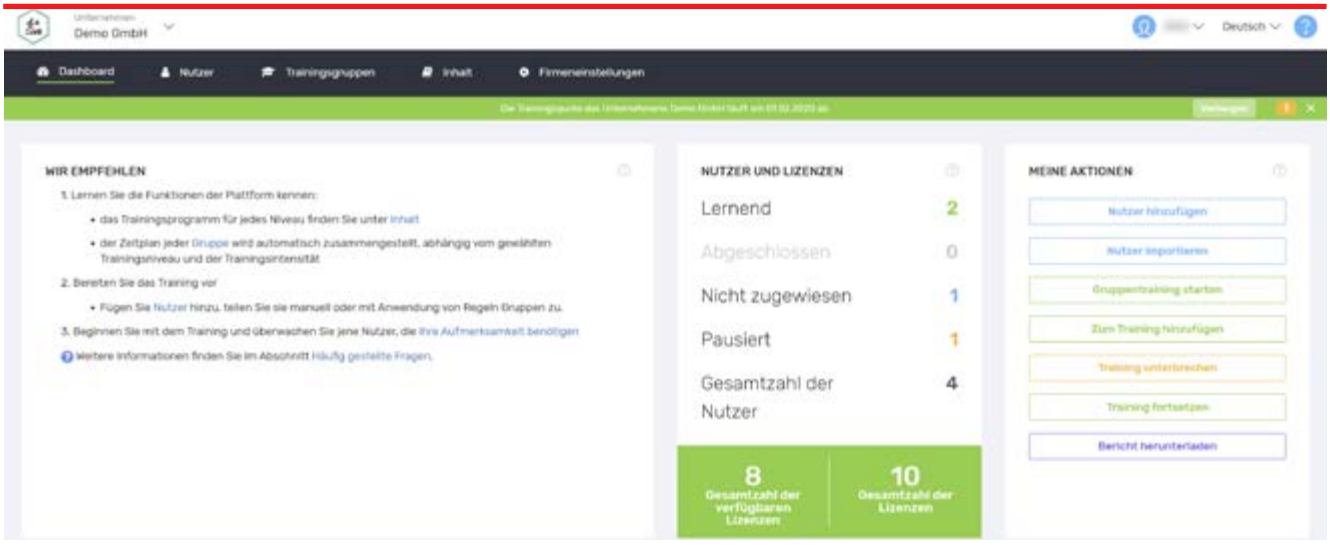
Bis zu **90%** Reduzierung der IT-Sicherheitsvorfälle

Bis zu **50%** Reduzierung der Kosten von IT-Sicherheitsvorfällen

Bis zu **93%** Erfolgsquote, dass das Wissen im Alltag angewendet wird

Bis zu **86%** der Teilnehmer empfehlen Security Awareness Trainings weiter

Mehr als **30%** ROI



KASPERSKY INTERACTIVE PROTECTION SIMULATION

KIPS

DAS PLANSPIEL KIPS FÖRDERT AUF SPIELERISCHE WEISE DIE STRATEGISCHEN ENTSCHEIDUNGEN UND KENNTNISSE RUND UM CYBERSECURITY.

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.

Gemeinsam mit den Teammitgliedern versuchen die Spieler, das Spiel mit maximalem Gewinn und einem funktionierenden Unternehmen zu beenden. Dies gelingt nur mit der Auswahl der besten verfügbaren, vorausschauenden Reaktionen auf die eintretenden Ereignisse des Spiels. Jede Entscheidung, jedes Ereignis verändert den Verlauf des Szenarios und damit den Gewinn bzw. den Verlust des Unternehmens.

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 und Know-how zum Aufbau der eigenen Cybersicherheitsstrategie an die Hand zu geben.

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

DAS ERWARTET DIE MITSPIELER

- Unerwartete, fortschrittliche Bedrohungen geben Einblicke, wie Kriminelle technisch vorgehen (Threat Intelligence) und welche Ziele sie verfolgen
- Vorfallsreaktion und Vorfallsprävention richtig kombinieren lernen
- Auswirkungen falsch konfigurierter Sicherheitskontrollen erleben
- Sensibililierung für gleichzeitige Warnsignale in Sicherheit, IT und Business

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.

BRANCHENBEZOGENE KIPS-SZENARIEN – WELCHE 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
  Die Folgen zahlreicher Bedrohungen kennenlernen – von Website Defacement über aktuelle Ransomware bis hin zu durchdachten APTs

CYBERSECURITY FOR IT ONLINE

CITO

CITO BIETET INTERAKTIVES TRAINING FÜR IT-GENERALISTEN, WIE 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.

Die meisten Unternehmen, die Awareness-Schulungen nutzen, bieten zweischichtige Cybersecurity-Schulungen an: Expertenschulungen für IT-Sicherheitsteams und Schulungen zur Verbesserung des Sicherheitsbewusstseins für Nicht-IT-Mitarbeiter. So lassen sich nachweislich die besten Ergebnisse, also maximaler Schutz (in Verbindung mit technischen Maßnahmen) gewährleisten.

AUFBAU & INHALT

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. Dabei lernen die Teilnehmer u. a.:

- Überprüfen von Vorfällen im Zusammenhang mit Malware
- Erstellen von Skripten zum Entfernen von Malware
- Das Arbeiten mit Systemen und Sandboxing-Lösungen sowie das Entfernen unerwünschter Programme und Dateien
- Durchführung von Netflow-Datenverkehrs-, Zeitachsen- und Ereignisprotokollanalysen
- Suchen und Entfernen von Phishing-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

KENNEN SIE SICH AUS MIT DEN GÄNGIGEN INCIDENTS?

KLASSIFIZIERUNG BEKANNTER BEDROHUNGEN

Bedrohungsklasse	Typ	Beschreibung
Abusive Content	Spam	or "Unsolicited Bulk Email", this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having a functionally comparable content
	Harmful Speech	Discreditation or discrimination of somebody (e.g. cyber stalking, racism and threats against one or more individuals)
	Child/Sexual/ Violence/	Child pornography, glorification of violence, ...
Malicious Code	Virus	Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.
	Worm	
	Trojan	
	Spyware	
	Dialler	
	Rootkit	
Information Gathering	Scanning	Attacks that send requests to a system to discover weak points. This includes also some kind of testing processes to gather information about hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, ...), port scanning.
	Sniffing	Observing and recording of network traffic (wiretapping).
	Social engineering	Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats).
Intrusion Attempts	Exploiting known vulnerabilities	An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as CVE name (e.g. buffer overflow, backdoor, cross site scripting, etc.).
	Login attempts	Multiple login attempts (guessing/cracking of passwords, brute force).
	New attack signature	An attempt using an unknown exploit.

Intrusions	Privileged account compromise	A successful compromise of a system or application (service). This can have been caused remotely by a known or new vulnerability, but also by an unauthorized local access. Also includes being part of a botnet.
	Unprivileged account compromise	
	Application compromise	
	Bot	
Availability	DoS	By this kind of an attack a system is bombarded with so many packets that the operations are delayed or the system crashes. DoS examples are ICMP and SYN floods, teardrop attacks and mail-bombing. DDoS often is based on DoS attacks originating from botnets, but also other scenarios exist like DNS Amplification attacks. However, the availability also can be affected by local actions (destruction, disruption of power supply, etc.) – or by Act of God, spontaneous failures or human error, without malice or gross neglect being involved.
	DDoS	
	Sabotage	
	Outage (no malice)	
Information Content Security	Unauthorised access to information	Besides a local abuse of data and systems the information security can be endangered by a successful account or application compromise. Furthermore, attacks are possible that intercept and access information during transmission (wiretapping, spoofing or hijacking). Human/configuration/software error can also be the cause.
	Unauthorised modification of information	
Fraud	Unauthorized use of resources	Using resources for unauthorized purposes including profit-making ventures (e.g. the use of e-mail to participate in illegal profit chain letters or pyramid schemes).
	Copyright	Offering or installing copies of unlicensed commercial software or other copyright protected materials (Warez).
	Masquerade	Type of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it.
	Phishing	Masquerading as another entity in order to persuade the user to reveal a private credential.
Vulnerable	Open for abuse	Open resolvers, world readable printers, vulnerability apparent from Nessus etc scans, virus signatures not up-to-date, etc
Other	All incidents which do not fit in one of the given categories should be put into this class.	If the number of incidents in this category increses, it is a indicator that the classification scheme must be revided.
Test	Meant for testing	Meant for testing

Quelle: eCSIRT.net mkVI

8Soft GmbH
Prymstraße 3
D-97070 Würzburg

+49 931 250993-20
info@8soft.de

www.8soft.de

Experts Security Distribution

IT SECURITY, THAT'S US!