SIMPLYIT
LANWORKS

WIR MACHEN EXPERTENWISSEN WIRKSAM

www.lanworks.de

Halloween ist in der Softwarebranche das ganze Jahr…

Der BSI-Bericht zur Lage der IT-Sicherheit in Deutschland 2021 zeigt alarmierendes Bild

Am letzten Wochenende war es mal wieder soweit - Halloween war angesagt und es gab viel Anlass, sich zu gruseln – vor den Gespenstern, Vampiren oder Hexen, die ihr Unwesen trieben und von Haus zu Haus zogen und nach Süßigkeiten fragten. Für reichlich Gruselfaktor - und das nicht nur an Halloween – sorgt aber auch ein Blick auf die steigende Zahl sowie die immer gravierenderen Folgen von Angriffen auf die IT-Sicherheit in Deutschland.

13 Tage lang musste das Universitätsklinikum Düsseldorf die Notaufnahme schließen. Die Zeitungen der Funke Mediengruppe konnten knapp einen Monat lang nur im Notbetrieb erscheinen. Das Umweltbundesamt musste seine komplette E-Mail-Infrastruktur neu aufbauen und war zwischenzeitlich nicht erreichbar.

Und nachdem Hacker am 15. Oktober die Stadtverwaltung von Schwerin mit einer Ransomware-Attacke gezwungen hatten, ihre IT-Systeme herunterzufahren, hat es kurz darauf auch die Stadt Witten in Nordrhein-Westfalen erwischt. Als in der Nacht zum Samstag des 16. Oktobers eine Cyber-Attacke bemerkt wurde, haben die Verantwortlichen alle betroffenen Systeme heruntergefahren und die Verwaltung in einigen Teilen auf Analogbetrieb umgestellt, um zumindest eine Art Notbetrieb am Laufen zu halten.

Lanworks AG
IT Engineering • IT Training & Coaching
Hellersbergstraße 10A • 41460 Neuss
Fon +49 211 95059-69

Die IT ist aber auch Tage nach dem Angriff immer noch lahmgelegt. Im Jahr 2021 sind nun schon 22 öffentliche Verwaltungen von einem Hackerangriff betroffen.

Ein Rückblick auf die vergangenen zwölf Monate zeigt, dass die Bedrohung durch Cyber-Kriminelle für eine digitale Gesellschaft weiter ansteigt. Zu diesem Fazit kommt auch der Bericht zur Lage der IT-Sicherheit in Deutschland 2021, den das Bundesamt für Sicherheit in der Informationstechnik (BSI) Ende des Monats vorgestellt hat. Cyberangriffe in Deutschland, nicht nur mit dem Ziel das öffentliche Leben lahm zu legen, nehmen weiter zu und betreffen Unternehmen branchenübergreifend jeglicher Größe.

Immer häufiger verschlüsseln Kriminelle die Daten von Unternehmen und Institutionen in ausgefeilten mehrstufigen Angriffen, um Lösegeld zu erpressen. Auch der Umgang mit Schwachstellen ist und bleibt nach wie vor eine der größten Herausforderungen der Informationssicherheit. Und gibt es auch noch einen weiteren alten Bekannten: den Risikofaktor Mensch. Laut dem Report hat die Angreiferseite die Unsicherheit und Überforderung durch die Pandemie, den realen und empfundenen Zeitdruck sowie die gesellschaftliche und mediale Dominanz des Themas ausgenutzt, um Opfer durch Phishing-Angriffe und andere Betrugsformen zur Herausgabe sensibler Informationen oder personenbezogener Daten zu bewegen. Hinzu kamen weitere Faktoren wie Daten-Leaks, Angriffe auf Videokonferenzen, schlecht abgesicherte VPN-Server oder der Einsatz privater IT im beruflichen Kontext (BYOD).

Der Faktor Mensch – und wie Sie durch Cyber-Awareness Training die Sicherheit deutlich erhöhen können

Um die IT-Sicherheit nachhaltig zu verbessern ist Cyber-Awareness gefragt: In etwa 80% aller Cybersicherheitsvorfällen wird der Schaden durch menschliches Fehlverhalten, wie Unkenntnis und mangelndem Problembewusstsein verursacht. Das kann sich auf verschiedenen Ebenen abspielen: von der Verwendung unzureichender Passwörter, über sehr gut gemachte Phisingmails 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.

Lassen Sie Ihre Mitarbeiter nicht im Dunkeln tappen, sondern erhöhen Sie die Cyber-Awareness – mit zertifiziertem Training und Workshops

Um Wissen und dessen Anwendung im Alltag zu etablieren, reicht die bloße Existenz von Richtlinien und Regelwerken zum Umgang mit IT-Sicherheit nicht aus. Ein fundamentaler Baustein für den richtigen Umgang mit IT-Sicherheit ist daher die dauerhafte Sensibilisierung der Mitarbeiter für sicherheitsrelevante Themen.

Wie kann die Lanworks AG Sie unterstützen?

Die Lanworks AG kann auf Basis ihrer langjährigen Erfahrung im Kampf gegen Cyberkriminelle ein umfassendes Trainingsangebot für Angestellte realisieren. Den individuellen Trainingspfad zu finden, gehört seit fast 20 Jahren zu unseren täglichen Aufgaben. Wir entwickeln gemeinsam mit Ihnen Schulungskonzepte und -programme, die passen. Als Spezialisten beraten wir Sie gerne in allen Fragen zu Lernpfaden und Schulungsthemen. Unsere Trainingsberater nehmen sich auch gerne Zeit für Ihr individuelles Anliegen.

Rufen Sie sie einfach an unter [0211 950590] oder senden Sie eine E-Mail an sales@lanworks.de

Entdeckungsreise IT Trainings

Gehen Sie doch gleich auf Entdeckungsreise und erkunden Sie HIER unsere Welt der IT-Trainings!
Wählen Sie Ihr beliebtes Kursformat! Von IT-Kursen Online, Hybridtrainings, IT-Fortbildungen in Düsseldorf bis hin zu Inhouse-Schulungen ist alles möglich.

Lanworks AG
IT Engineering • IT Training & Coaching
Hellersbergstraße 10A • 41460 Neuss
Fon +49 211 95059-69