Bestens vorbereitet auf den Ernstfall.

Security Training im A1 Cyber Range Trainingscenter.

Im A1 Cyber Range Trainingscenter in Wiener Neustadt werden in realistischen Live-Szenarien Cyberattacken simuliert. In Gruppen von jeweils 6 Teilnehmern lernen IT-Spezialisten unter professioneller Anleitung auf die Bedrohungen schnell und zielgerichtet zu reagieren. In vorkonfigurierten oder frei gestaltbaren Umgebungen stehen Security Szenarien für IT und SCADA/ICS Systemen zur Verfügung. Diese können mit verschiednen Trainingsmodulen auf virtuellen Systemen trainiert werden.

Einfach besser geschützt.

Mehr Informationen zu A1 Cyber Range erhalten Sie unter **A1.net/cyberrange**

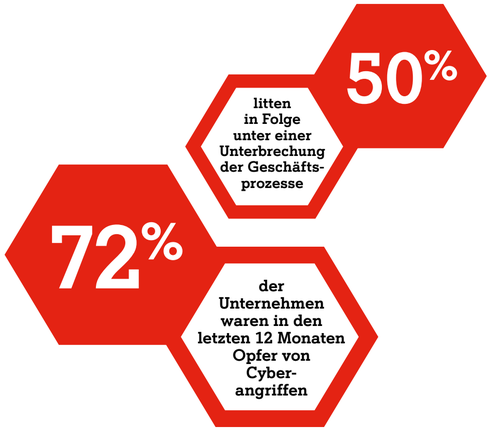
Im Zeitraum von 12. April bis 10. Mai 2017 wurden 236 österreichische Unternehmen von KPMG befragt, wie sie den Herausforderungen durch Cyberkriminalität begegnen und welche Cyber Security-Maßnahmen sie treffen. Die Umfrage wurde mit freundlicher Unterstützung des Kuratoriums Sicheres Österreich (KSÖ) durchgeführt und kann per E-Mail an publikationen@kpmg.at angefordert werden.

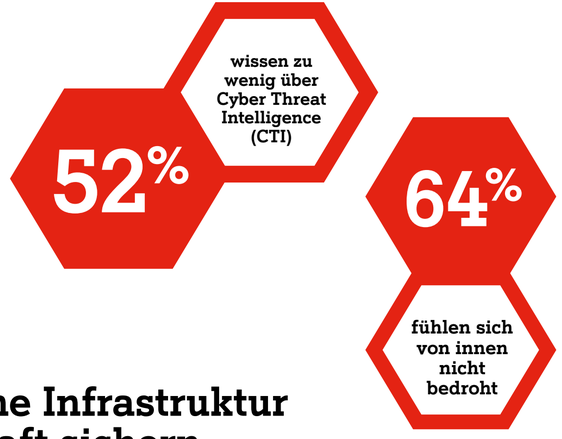
Vorbehaltlich Satz- und Druckfehler. Stand: August 2018.

(N851)
1-400-003-190 (gültig ab 17.09.2018)

Ich kann

alles





Mehr Cyber Security.

Ich kann Wertvolles richtig schützen.

Unser Leben ist von Technik und IT bestimmt. Überall unterstützen technische Geräte und digitale Systeme unseren Alltag. Werden diese Maschinen und Netzwerke Opfer von Cyberattacken, wird unser gewohntes Leben empfindlich gestört.

Um Unternehmen mit einer gut ausgebauten IT-Infrastruktur vor Attacken aus dem Internet zu schützen und ihre gut ausgebildeten IT-Spezialisten für die Zukunft noch besser vorzubereiten, bietet A1 jetzt die Möglichkeit, den Ernstfall einer Cybercrime-Attacke zu trainieren. Mit A1 Cyber Range.

Mehr Fortbildung.

Ich kann den Ernstfall üben.

A1 Cyber Range ist eine Trainingsplattform, mit der IT- und SCADA/ICS- Spezialisten Cyberattacken in gesichertem Umfeld simulieren und lösen können. Und so mit Stresstest die Cyber Security in ihrem Unternehmen erhöhen. Sie unterstützen dadurch die Umsetzung der EU Empfehlungen und Richtlinien und tragen so zum Schutz von Betreiber kritischer Infrastruktur bei.

Individuelle und dynamische Netzwerkabbildungen sorgen dabei für eine realistische Simulation einer Vielfalt möglicher Gefahren, Bedrohungen und Attacken. In maßgeschneiderten und adaptierbaren Modulen erhalten die IT-Experten Echtzeit-Feedback von den Security-Experten von A1.

Bedrohungen rechtzeitig erkennen.

Für mehr Sicherheit in Unternehmen.

Fließendes Wasser, Strom und eine funktionierende Gesundheitsversorgung: Wir sind auf das Bestehen zahlreicher technischer und digitaler Systeme angewiesen. Was es bedeutet, wenn grundlegende Bereiche des modernen Lebens nicht mehr bereitstehen, kann jeder nachvollziehen, bei dem schon einmal der Strom ausgefallen ist.

Mögliche Bedrohungsszenarien durch Cyberattacken gibt es viele: Medien berichten immer häufiger von Cyberattacken, Phishing-Versuchen und anderen Angriffen auf die Sicherheit kleiner und großer Unternehmen. Experten schätzen den Schaden, der dadurch entsteht, auf 400 bis 500 Milliarden Euro.

Vielleicht haben Sie selbst schon einmal einen Angriff miterlebt oder längere Ausfallzeiten und Datenverlust nach einem solchen Vorfall verkraften müssen. Mit A1 haben Sie einen Partner an der Hand, der Sie vor solchen Szenarien schützt.

Aber auch in Unternehmen können Cyberangriffe massive Schäden anrichten. Zwar sind etwa Online-Marktplätze oder Suchmaschinen nicht Teil der Grundversorgung, doch auch Unternehmen und Bürger sind vom reibungslosen Funktionieren des Internets abhängig.

Kritische Infrastruktur dauerhaft sichern.

Und die Abwehrfähigkeit gegenüber Cyberangriffen stärken.

Sensible Bereiche des Wirtschaftslebens und der allgemeinen Infrastruktur eines Staates bedürfen besonderer Sicherheitsmaßnahmen. A1 Cyber Range bietet die Möglichkeit, den Ernstfall zu trainieren. Damit, wenn es notwendig wird, präventiv gegen Sicherheitsvorfälle, die Netz- und Informationssysteme betreffen, vorgegangen und rasch und professionell darauf reagiert werden kann.

Mit der NIS-Richtlinie der EU werden neben staatlichen Stellen auch zahlreiche Unternehmen in die Verantwortung genommen. Um EU-weit ein hohes Niveau der Netz- und Informationssysteme zu erreichen, sollen etwa Unternehmen aus wirtschaftlich oder gesellschaftlich besonders wichtigen Bereichen adäquate Sicherheitsmaßnahmen einführen. Dazu zählen Betreiber wesentlicher Dienste wie Energie, Transportwesen, Finanzwirtschaft, Gesundheitsversorgung, Wasserversorgung und digitale Infrastruktur.

Die Richtlinie verfolgt dabei die Stärkung der Kapazitäten der Mitgliedstaaten im Bereich der Cybersicherheit, den Ausbau der Zusammenarbeit auf EU-Ebene und die Förderung einer Kultur des Risikomanagements und der Meldung von Sicherheitsvorfällen bei zentralen Wirtschaftsakteuren. Auch im Regierungsprogramm 2017-2022 wird dem Schließen von Sicherheitslücken digitaler Netze große Bedeutung eingeräumt.