New Horizons®

Cybersecurity: Deine Rolle für den Schutz deines Teams

Mach dein Team fit für einen sicheren digitalen Arbeitsalltag!

New Challenge. New Skills. New You.

Stärke dein Team:
Mach Cybersicherheit zu einem festen Bestandteil des Arbeitsalltags.

Digitale Informationen und Technologien gehören heute ganz selbstverständlich zum Arbeitsalltag.

Umso wichtiger ist es, aufmerksam zu bleiben und Cybersicherheit im täglichen Arbeiten mitzudenken.

Social Engineering wird immer raffinierter. Oft reicht eine überzeugend formulierte E-Mail oder ein scheinbar vertrauter Link, um jemanden zu einer unbedachten Aktion zu verleiten. Mit dem richtigen Wissen und einem bewussten Umgang mit digitalen Inhalten kannst du solche Situationen besser einschätzen und sicher reagieren.

Drei Bereiche, die für Cybersicherheit entscheidend sind:

Menschen:
95 % aller Datenlecks sind auf menschliches Versagen zurückzuführen. Dein Verhalten macht deshalb einen echten Unterschied. Wenn du aufmerksam handelst und Sicherheitsregeln im Alltag berücksichtigst, kannst du dazu beitragen, Sicherheitsvorfälle und ihre Auswirkungen zu reduzieren.

Prozesse:
Klare und gut durchdachte Abläufe helfen dabei, auf neue Herausforderungen flexibel zu reagieren. Gleichzeitig sorgen sie dafür, dass du deine Rolle und Verantwortung im Umgang mit Cybersicherheit kennst.

Technologie:
Neue Technologien eröffnen viele Möglichkeiten, bringen aber auch neue Sicherheitsfragen mit sich. Phishing, Datenlecks oder Schwachstellen in digitalen Systemen zeigen, wie wichtig ein bewusster und sicherer Umgang mit Technologie ist.

Jedes Element spielt eine entscheidende Rolle beim Aufbau einer robusten Cybersicherheitsstrategie.

Ein integrierter Ansatz stärkt nicht nur die Widerstandsfähigkeit gegen Sicherheitsverletzungen, sondern fördert auch eine Kultur des Sicherheitsbewusstseins im gesamten Unternehmen und stellt sicher, dass alle Mitarbeiter in der Lage sind, sich in der sich ständig verändernden Bedrohungslandschaft zurechtzufinden.

Versteckte Risiken am Arbeitsplatz.

Da der Einsatz von KI in Ihrem Unternehmen immer mehr zur Selbstverständlichkeit wird, ist es entscheidend, die damit verbundenen Risiken zu erkennen. Ohne angemessene Aufsicht und Schulung der Mitarbeiter birgt KI zahlreiche Risiken, darunter:

- Offenlegung sensibler Daten durch KI-gestützte Erkenntnisse
- Unbefugter Zugriff auf KI-basierte Systeme
- Falsche Konfiguration von KI-Sicherheitstools

Die Zahlen hinter den digitalen Risiken

Digitale Sicherheit gehört heute zum Arbeitsalltag. Je besser du typische Risiken kennst, desto leichter kannst du aufmerksam handeln und zu einem sicheren Umgang mit Daten und Technologien beitragen. Diese Infografik gibt dir einen kompakten Überblick über ausgewählte Zahlen und Entwicklungen.

Cyberrisiken in Zahlen (am Beispiel US)

Alle 39 Sekunden findet laut Quelle ein Hackerangriff statt.
70 %der Phishing-E-Mails sind KI-generiert oder mithilfe von KI optimiert.
50.000 Websites werden laut Quelle täglich gehackt.
300.000 neue Schadprogramme entstehen laut Quelle jeden Tag.

Warum sich Cybersicherheit lohnt

95 % der Datenschutzverletzungen werden laut Quelle auf menschliche Fehler zurückgeführt.
93 % der Organisationen erwarten höhere Ausgaben für Cybersicherheit im kommenden Jahr.
55 % der Unternehmen planen mehr Investitionen in KI-gestützte
9,36 Mio. US-Dollar betrugen 2024 laut Quelle die durchschnittlichen Kosten einer Datenschutzverletzung in den USA.

Cybersicherheit: ein Feld mit Zukunft

3,5 Mio.Stellen im Bereich Cybersicherheit sollten laut Schätzung bis Ende 2025 unbesetzt bleiben.
2,22 Mio. US-Dollar durchschnittliche Kostenersparnis durch KI und Automatisierung in der Sicherheit.
60 % der Organisationen sollten Zero Trust bis 2025 als Ausgangspunkt ihrer Sicherheitsstrategie einsetzen.
33 % Wachstum wurde für den Cybersicherheitsmarkt zwischen 2021 und 2031 erwartet.

Quelle: © New Horizons Worldwide, LLC. All rights reserved. 1 Watters, A. (2023, January 27). Top 50 Cybersecurity Statistics, Figures and Facts. Default. https://connect.comptia.org/blog/cyber-security-stats-facts 2 James, N. (2023, May 2). 160 Cybersecurity Statistics 2023 - The Ultimate List of Stats and Trends. Astra Security Blog. https://www.getastra.com/blog/security-audit/cyber-security-statistics/#:~:text=Cybersecurity%20statistics%20indicate%20that%20there, cost%20%248%20trillion%20by%202023 3 The CISO Report. Splunk, Splunk Inc., www.splunk.com/en_us/campaigns/ciso-report.html. 4Cybereason Blog. https://www.cybereason.com/ 5Deloitte. 2021 Future of Cyber Survey. Deloitte, 2021, https://www2.deloitte.com/us/en/pages/advisory/articles/future-of-cyber-survey.html. 6IBM. Cost of a Data Breach Report 2024. IBM Security, 2024, www.ibm.com/reports/data-breach. 7 Gopal, D. McMullen, L. (2023, January 25). Predicts 2023: Cybersecurity Industry Focuses on the Human Deal. Gartner, https://www.gartner.com/doc/reprints?id=1-2D7XIUC3&ct=230413&st=sb 8Mastercard. Trust Center: Small Business Cyber Safety Starts with the Basics. Mastercard,https://www.mastercard.us/en-us/business/overview/safety-and-security/trust-center.html. www.ibm.com/reports/data-breach. 7 Gopal, D. McMullen, L. (2023, January 25). Predicts 2023: Cybersecurity Industry Focuses on the Human Deal. Gartner. https://www.gartner.com/doc/reprints?id=1-2D7XIUC3&ct=230413&st=sb 8Mastercard. Trust Center: Small Business Cyber Safety Starts with the Basics. Mastercard, https://www.mastercard.us/en-us/business/overview/safety-and-security/trust-center.html.

Bewährte Verfahren für Cybersicherheit

Cybersicherheit geht jeden etwas an und spielt eine entscheidende Rolle bei der Aufrechterhaltung einer starken Cybersicherheitslage. Hier sind einige proaktive Ansätze für kontinuierliche Sicherheit:

Bleib auf dem Laufenden:
Informiere dich regelmäßig über aktuelle Entwicklungen und bewährte Methoden rund um Cybersicherheit. Wenn du typische Risiken kennst, kannst du im Arbeitsalltag sicherer damit umgehen.

Nutze sichere und einzigartige Passwörter:
Verwende für jedes Konto ein eigenes, sicheres Passwort. Eine Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen erhöht die Sicherheit. Ein Passwort-Manager hilft dir dabei, deine Passwörter sicher zu speichern und zu verwalten.

Achte auf Phishing:
Schau bei ungewöhnlichen E-Mails lieber einmal genauer hin. Prüfe Absender, Links und Anhänge, besonders wenn du zur Eingabe persönlicher Daten aufgefordert wirst. Bist du dir unsicher, überprüfe zunächst, ob die Nachricht wirklich von der angegebenen Person oder Organisation stammt.

Halte deine Software aktuell:
Installiere regelmäßig Updates für dein Betriebssystem, deine Anwendungen und deine Sicherheitssoftware. So bleiben wichtige Sicherheitspatches auf dem neuesten Stand und bekannte Schwachstellen werden geschlossen.

Schütze deine Geräte:
Sichere deine Arbeitsgeräte mit einem starken Passwort oder biometrischer Authentifizierung. Nutze außerdem Bildschirmsperre und Verschlüsselung sowie – wenn verfügbar – Funktionen zur Fernortung und zum Löschen von Daten.

Surfe sicher:
Nutze für Online-Transaktionen nur vertrauenswürdige Websites. Sei bei unbekannten Seiten, Links und Downloads aufmerksam und lade keine Dateien aus Quellen herunter, denen du nicht vertraust.

Geh bewusst mit sozialen Medien um:
Überlege dir gut, welche persönlichen oder sensiblen Informationen du teilst. Frag dich im Zweifel: Wäre es für mich in Ordnung, wenn diese Information öffentlich wäre? Prüfe auch deine Datenschutzeinstellungen und passe sie bei Bedarf an.

Melde Sicherheitsvorfälle:
Kommt dir etwas verdächtig vor – zum Beispiel eine Phishing-Mail, Malware oder ein möglicher unbefugter Zugriff –, melde es direkt deinem IT-Support-Team. Je früher dein Team Bescheid weiß, desto schneller kann es reagieren.

Kontinuierliche Schulungen und Unterstützung

Als erste Verteidigungslinie gegen Cyberangriffe spielen Mitarbeiter eine entscheidende Rolle beim Schutz sensibler Informationen und bei der Wahrung der Integrität des Unternehmens.

Du bist ein wichtiger Teil der Cybersicherheit in deinem Unternehmen. Mit deinem Verhalten im Arbeitsalltag trägst du dazu bei, sensible Informationen zu schützen und Sicherheitsrisiken frühzeitig zu erkennen.

Regelmäßige Schulungen helfen dir und deinem Unternehmen dabei, typische Risiken wie Phishing oder Social Engineering besser zu erkennen und in solchen Situationen richtig zu reagieren.

Denk daran: Cybersicherheit ist Teamarbeit! Wenn wir alle aufmerksam bleiben und ein paar einfache Sicherheitsregeln zur Gewohnheit machen, schaffen wir gemeinsam ein sichereres Arbeitsumfeld.

Cybersecurity Trainings bei New Horizons

Entdecke die Cybersicherheitsschulungen von New Horizons und finde das passende Angebot für dich und dein Team.

Wir unterstützen dich dabei, Wissen aufzubauen, Sicherheit im digitalen Arbeitsalltag zu gewinnen und dein Team gut auf aktuelle Herausforderungen vorzubereiten.

Kurse sind online verfügbar, flexibel und praxisnah. Wer regelmäßig übt, reagiert schneller auf Bedrohungen und nutzt Technik sicherer.

So wird IT-Sicherheit verständlich und greifbar – für alle Berufsgruppen.

Du möchtest mehr erfahren?

Das QCG-Programm. Für alle . Unternehmen.

Der Bund fördert Eure Weiterbildung bis zu 100%!

Deine Chance auf Weiterbildung bei New Horizons: alle Kurse sind bis zu 100% föderbar!

Das Qualifizierungschancengesetz

Entfalte dein Potenzial mit dem Qualifizierungschancengesetz für deine berufliche Zukunft und nutze die Chancen einer gezielten Weiterbildung! Unsere exklusive Weiterbildungsmaßnahmen bieten Dir nicht nur hochwertiges Fachwissen, sondern ermöglicht dir die finanzielle Unterstützung durch die QCG Förderung (Qualifizierungschancengesetz).

Wie funktioniert die QCG Förderung?

Das Qualifizierungschancengesetz bietet finanzielle Mittel für die Weiterbildung von Arbeitnehmern. Wir helfen dir, die Fördermittel zu beantragen, damit du dich auf das konzentrieren kannst, was wirklich wichtig ist – deine Weiterbildung und berufliche Entwicklung.

Wie kann ich die QCG-Budgetlösung für mich und mein Unternehmen nutzen?

Kontaktiere uns noch heute, um mehr über unsere Weiterbildungsmaßnahme und die Möglichkeiten der finanziellen Unterstützung zu erfahren:

Beratungstermin vereinbaren