# Cyber Security in Österreich

Cyberkriminalität ist ein globales Milliardengeschäft, auch mit Opfern in Österreich. Zahlen und Fakten sind wichtige Elemente, um einen Gesamtüberblick über die „Lage der Nation" in Sachen Cyberangriffe und -sicherheit zu erhalten. Darum hat KPMG bereits zum dritten Mal die Umfrage „Cyber Security in Österreich" durchgeführt.

Die Zahlen verraten Trends und Veränderungen, machen deutlich, wo es Nachholbedarf gibt und in welchen Bereichen die Alpenrepublik bereits gut aufgestellt ist. Sie sind eine entscheidende Diskussionsgrundlage und Basis für weitere Aktivitäten.

**Next Level: Der digitale Wirtschaftsstandort**

Doch nun müssen den Zahlen Taten folgen. Das übergeordnete Ziel für unser Land sollte sein, eine wirksame Strategie zur Bekämpfung von Cyberrisiken zu entwickeln. Dafür muss, eine Basis für einen erfolgreichen Digital-Wirtschaftsstandort Österreich geschaffen werden. Unser Land weist hervorragende „analoge" Qualitäten, wie Rechtssicherheit und Stabilität auf. Diese Eigenschaften gilt es für das digitale Zeitalter zu adaptieren, um den Wirtschaftsstandort Österreich zu sichern.

Um das zu erreichen, müssen sinnvolle und strategische Maßnahmen ausgearbeitet werden. Dabei sind die einzelnen Unternehmen genauso gefragt wie staatliche Organisationen. Denn: Im Bereich Cyber sitzen alle Akteure in einem Boot, jeder Einzelne muss daher seine Verantwortung wahrnehmen. Eine gemeinsame Strategie erfordert eine Zusammenarbeit, einen Gedanken- und Informationsaustausch. Denn der Kampf gegen Cyberkriminalität ist nur gemeinsam zu gewinnen. Dieses Bewusstsein hat sich hierzulande bereits bis zu einem gewissen Grad durchgesetzt: zahlreiche Kooperationen setzen aktiv Zeichen.

**Falsch gelegen: Die größten Irrtümer**

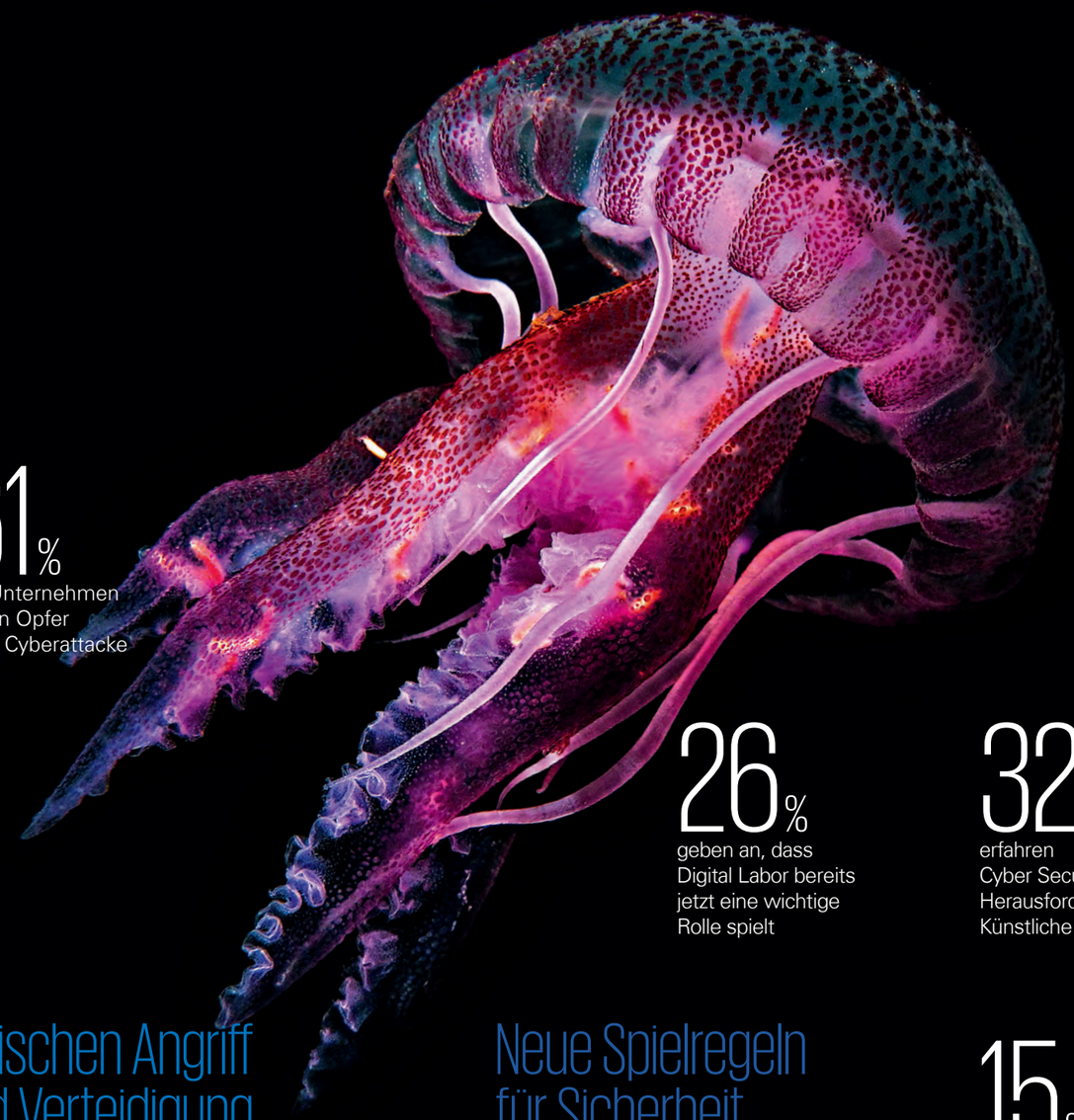
Nach wie vor herrschen zahlreiche Missverständnisse rund um Cyber Security. Diese führen wiederum zu strategisch unklugen Entscheidungen in Unternehmen. Eine der größten Fehlannahmen ist die Vision, 100 prozentige Cybersicherheit anzustreben. Ein solcher Schutz vor Cyberkriminalität ist weder machbar noch ein geeignetes Ziel. Der zielgerichtete Schutz besonders wertvoller Informationen ist der richtige Weg und wird aufgrund der schier unermesslichen Datenflut für Unternehmen entscheidend.

Ein weiterer Irrtum ist die Annahme, dass die Implementierung der besten erhältlichen Sicherheitstools entscheidend für Cybersicherheit ist. Die technischen Werkzeuge sind für die Basissicherheit unerlässlich. Leider herrscht noch allzu oft die Annahme vor, Cybersicherheit sei ein rein technisches Thema. IT-Tools sind aber nur ein Teil und nicht die Grundlage einer ganzheitlichen Cyber Security-Politik. Unternehmen müssen einen strategischen Maßnahmen-Mix umsetzen, der Technologien, Menschen und Prozesse gleichermaßen berücksichtigt. Wichtig dabei: Cybersicherheit muss ein Thema der Chefetage sein und von dort aus gesteuert werden. Dies ist, angesichts der Komplexität der Technologie und des Tempos der Veränderung, keine leichte Aufgabe.

Manche Unternehmen glauben fälschlicherweise: „Wir stellen die besten Experten an, um uns gegen Cyberkriminalität zu schützen." Natürlich ist es wichtig, Experten zu beschäftigen. Doch die eigentliche Herausforderung ist es, Cybersicherheit zu einem Mainstream-Ansatz im Unternehmen zu machen. Cyber Security muss zu einem Teil der organisationsweiten Vorgaben und Richtlinien werden und vollinhaltlich in die Unternehmensziele integriert werden.

# Cyber Security in Österreich

**Key Findings 2018**



## Tatort Internet

Österreichs Unternehmen im Visier

**60%** der Angriffe zielen auf die „Schwachstelle Mensch“

**61%** der Unternehmen waren Opfer einer Cyberattacke

**73%** fühlen sich in Cyber Security-Belangen wohl

**91%** haben ihr Verständnis für Cyberrisiken verbessert

## Wirksame Verteidigung

Künstliche Intelligenz bietet innovative Möglichkeiten

**26%** geben an, dass Digital Labor bereits jetzt eine wichtige Rolle spielt

**32%** erfahren Cyber Security-Herausforderungen durch Künstliche Intelligenz

## Zwischen Angriff und Verteidigung

Aktion & Reaktion der Unternehmen

**52%** prognostizieren einen Anstieg des Cyber Security-Budgets

**45%** melden cyberkriminelle Vorfälle nicht

## Neue Spielregeln für Sicherheit

Das Internet ist kein rechtsfreier Raum

**15%** sehen in der Löschung der Daten das größte Problem der DSGVO-Umsetzung

**74%** erwarten eine Zunahme der Kundenanfragen zum Datenschutz

## Mit Strategie zum Erfolg

Cyber Security als Chefsache

**45%** führen eine Messung der Cyber Security-Risiken mittels Kennzahlen durch

**79%** diskutieren Cyber Security-Themen auf oberster Unternehmensebene

## Auf neuen Wegen

Die Zukunft der Cyber Security in Unternehmen

**67%** der Unternehmen beklagen einen Mangel an Cyber Security-Experten

**49%** glauben, dass die Cloud-Nutzung den Infrastrukturaufwand verringert

* Im März und April 2018 wurden 269 österreichische Unternehmen von KPMG befragt, wie sie den Herausforderungen durch Cyberkriminalität begegnen und welche Cyber Security-Maßnahmen sie treffen. Die Umfrage wurde in Kooperation mit dem Sicherheitsforum des KSÖ (Kuratorium Sicheres Österreich) durchgeführt und kann per E-Mail an publikationen@kpmg.at angefordert werden.

## PRÄVENTION & SICHERHEIT

**Der Chef am Zug: Cybersicherheit in Unternehmen**
Cyberrisiken sind eine große Herausforderung für die Führung von Unternehmen. Die Entschuldigung, die Verantwortung den Experten zu überlassen, gilt nicht mehr. Es ist unerlässlich, dass die Unternehmensführung das Unternehmen in folgenden Bereichen lenkt und verantwortet:

- Zuteilung von Ressourcen, um Cyber Security betreiben zu können.
- Eine unternehmensweite Governance, die eine risikobasierte Entscheidungsfindung erlaubt.
- Eine Unternehmenskultur, in der jeder um seine Verantwortung weiß.

Unternehmen können die Risiken für ihr Geschäft durch den Aufbau von Kapazitäten in den folgenden drei kritischen Bereichen reduzieren:

- Prävention: strategische, taktische und technische Maßnahmen; Sensibilisierungsmaßnahmen
- Erkennung: Überwachung von kritischen Ereignissen und Sicherheitsvorfällen
- Reaktion: strukturierter Maßnahmenplan nach einem Angriff inklusive Wiederherstellungsplan

Für alle Maßnahmen zur Stärkung der eigenen Sicherheit sowie jener des Unternehmensstandorts Österreich gilt: Dem Thema Cyber Security muss sowohl innerhalb der Unternehmen als auch auf politischer Ebene die notwendige Bedeutung zukommen.

In Österreich ist man in Sachen Cybersicherheit auf dem richtigen Weg. Dennoch darf man sich nicht auf den bisherigen Lorbeeren ausruhen, sondern muss sich den kommenden Herausforderungen stellen.

Denn das Thema Cybersicherheit ist vor allem durch zwei Merkmale gekennzeichnet: Veränderung und Tempo.

**Gemeinsam Zukunft schreiben**
Finden Sie gemeinsam mit KPMG die richtige Strategie zur optimalen Umsetzung Ihres Cyber Security-Ansatzes. Mithilfe unseres exzellenten Know-hows und unserer jahrelangen Erfahrung entwickeln wir optimale Lösungen für eine verlässliche Cyber Security in Ihrem Unternehmen.

Sie können daraus auch einen echten strategischen Vorteil machen.

**Kontakt**


**Michael Schirmbrand**
Partner, Advisory
T +43 664 816 09 69
E mschirmbrand@kpmg.at

**Andreas Tomek**
Partner, Advisory
T +43 664 816 09 95
E atomek@kpmg.at

**Gert Weidinger**
Partner, Advisory
T +43 664 304 60 11
E gweidinger@kpmg.at

**Robert Lamprecht**
Director, Advisory
T +43 664 816 12 32
E rlamprecht@kpmg.at


**kpmg.at/cyber**

**Notfall-Hotline: 0800 07 10 30/cyber@kpmg.at**


© 2018 KPMG Security Services GmbH, österreichisches Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Printed in Austria. KPMG und das KPMG-Logo sind eingetragene Markenzeichen von KPMG International.

Die enthaltenen Informationen sind allgemeiner Natur und nicht auf die spezielle Situation einer Einzelperson oder einer juristischen Person ausgerichtet. Obwohl wir uns bemühen, zuverlässige und aktuelle Informationen zu liefern, können wir nicht garantieren, dass diese Informationen so zutreffend sind wie zum Zeitpunkt ihres Eingangs oder dass sie auch in Zukunft so zutreffend sein werden. Niemand sollte aufgrund dieser Informationen handeln ohne geeigneten fachlichen Rat und ohne gründliche Analyse der betreffenden Situation. Unsere Leistungen erbringen wir vorbehaltlich der berufsrechtlichen Prüfung der Zulässigkeit in jedem Einzelfall.