# Wer auf Nummer sicher gehen will, verankert eine Cybersecurity-Kultur

**Bei der Anzahl Cyberangriffe zeigt der Trend deutlich nach oben, seit Pandemiebeginn noch stärker. Technische Sicherheitsmassnahmen helfen. Entscheidend ist für ein Unternehmen aber das Verhalten der Mitarbeitenden und deshalb eine gut verankerte Cybersecurity-Kultur.**

Im Juni 2020 meldete Swissinfo.ch, dass sich die Anzahl Cyberangriffe in der Schweiz während der Covid-19-Pandemie gemäss dem National Cyber Security Center (NCSC) verdreifacht habe. Da es lange dauern kann, solche Angriffe zu entdecken, führen sie oft zu finanziellen Schäden, Wettbewerbsnachteilen und Vertrauensverlust.

Studien zeigen zudem, dass die meisten Cyberangriffe durch ungeschulte, unaufmerksame Mitarbeitende ermöglicht werden. Dennoch konzentrieren sich Unternehmen vor allem auf technische Sicherheitsmassnahmen wie Firewalls und Antivirus-Software. Dabei wäre eine gut etablierte Cybersecurity-Kultur zentral: Sie schärft das Bewusstsein für Gefahren und den Umgang damit.

### Wie etabliert man eine Cybersecurity-Kultur?

Eine Cybersecurity-Kultur entsteht nicht von allein, sondern erfordert gewisse Anstrengungen. Ein 5-Punkte-Plan:

### 1. Holen Sie die Unternehmensleitung an Bord

Die Unternehmensleitung muss sich zu einer Cybersecurity-Kultur bekennen, indem sie etwa durch Schulungen und Prozessanpassungen deren Bedeutung klar macht. Bilden Sie eine Sicherheitsorganisation, der zentrale Stakeholder wie die Unternehmensleitung, ein Sicherheitsbeauftragter und Information Asset Owner angehören. Um eine Cybersecurity-Kultur im Bewusstsein der Belegschaft zu verankern, müssen sie eng zusammenarbeiten.

### 2. Erlassen Sie klare Richtlinien

Erlassen Sie klare Richtlinien, die alle Mitarbeitenden zu beachten haben, wenn sie Informationen und IT-Geräte der Firma nutzen. Weisen Sie etwa darauf hin, dass die Nutzung von nicht vom Unternehmen bereitgestellter Hardware und Software untersagt ist. Die Erfahrung zeigt, dass das Fundament praktischer Massnahmen die Verantwortung ist. Deshalb müssen Verstösse angesprochen und geahndet werden – unabhängig von Rang oder Position einer Person.

### 3. Sensibilisieren Sie

Mitarbeitende müssen die Sicherheitsrichtlinien kennen, die für Firmen- und Kundeninformationen gelten. Nur so vermeiden Sie Datenlecks, die das Vertrauen in das Unternehmen erschüttern. Wichtig ist eine zielgruppengerechte Sensibilisierung. Wer mobile Geräte nutzt, sollte zum Beispiel über «Shoulder Surfing» Bescheid wissen und stets VPN nutzen. Prüfen Sie, ob die Massnahmen eingehalten werden.

### 4. Sorgen Sie für eine einfache Kommunikation

Die Kommunikation im Umgang mit Gefahren sollte eng koordiniert sein. Klare, einfache und für alle zugängliche Kanäle stellen sicher, dass Mitarbeitende verdächtige Aktivitäten zügig melden. Sollte sich eine solche Aktivität als harmlos herausstellen, verzichten Sie darauf, die betreffende Person zu kritisieren. Überlegen Sie sich, Cybersecurity ins jährliche Mitarbeitergespräch zu integrieren.

### 5. Testen Sie mit realen Szenarien

Tests und Übungen eignen sich bestens, um Mitarbeitende auf reale Angriffe vorzubereiten. Sie erkennen, wie gut sie im Ernstfall reagieren und was sie tun, um den Vorfall zu entschärfen. Es handelt sich hierbei um einen kontinuierlichen Lernprozess.

Wenn jeder Mitarbeitende geschult und sich der Risiken bewusst ist, profitiert das gesamte Unternehmen. Eine widerstandsfähige Sicherheitskultur ist Teil der Integrität eines Unternehmens. Die Cybersecurity-Kultur muss laufend geprüft, gestärkt und angepasst werden.

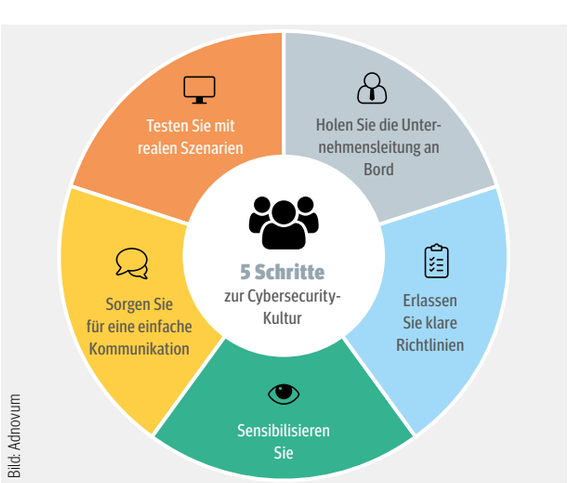


Bild: Adnovum

**DER AUTOR**

**Georges Eloundou Eloundou**
Senior Security Consultant, Adnovum

**Den Beitrag finden Sie auch online**
www.netzwoche.ch