PEN & PAPER
IT-SECURITY INCIDENT ÜBUNG

Steigerung der Cybersecurity durch realitätsnahe Simulation

sepago. making people love it.

"Unternehmen sind in der digitalen Welt zunehmend Cyberbedrohungen ausgesetzt, die schwer-wiegende Folgen haben können."

Die Bedeutung von Cybersecurity-Übungen für IT-Entscheidungsträger

In der heutigen digitalen Landschaft sind Unternehmen mehr denn je den Bedrohungen aus dem Cyberspace ausgesetzt. Cyberangriffe werden immer ausgefeilter und können verheerende Auswirkungen auf Geschäftsbetrieb, Datenintegrität und Kundenvertrauen haben. Es ist nicht die Frage ob, sondern wann ein Cyberangriff Ihr Unternehmen trifft. In diesem Kontext gewinnt die IT-Sicherheitsstrategie eine immense Bedeutung, und ein unverzichtbarer Bestandteil dieser Strategie sind Cybersecurity-Übungen. Aus diesem Grunde empfehlen wir die Notwendigkeit von Pen & Paper IT Security Incident Prozess-Übungen, die sowohl von der ISO 27001 als auch von Cybersecurity-Versicherungen gefordert werden.

Warum sind Cybersecurity-Übungen notwendig?

ISO 27001-Anforderungen:

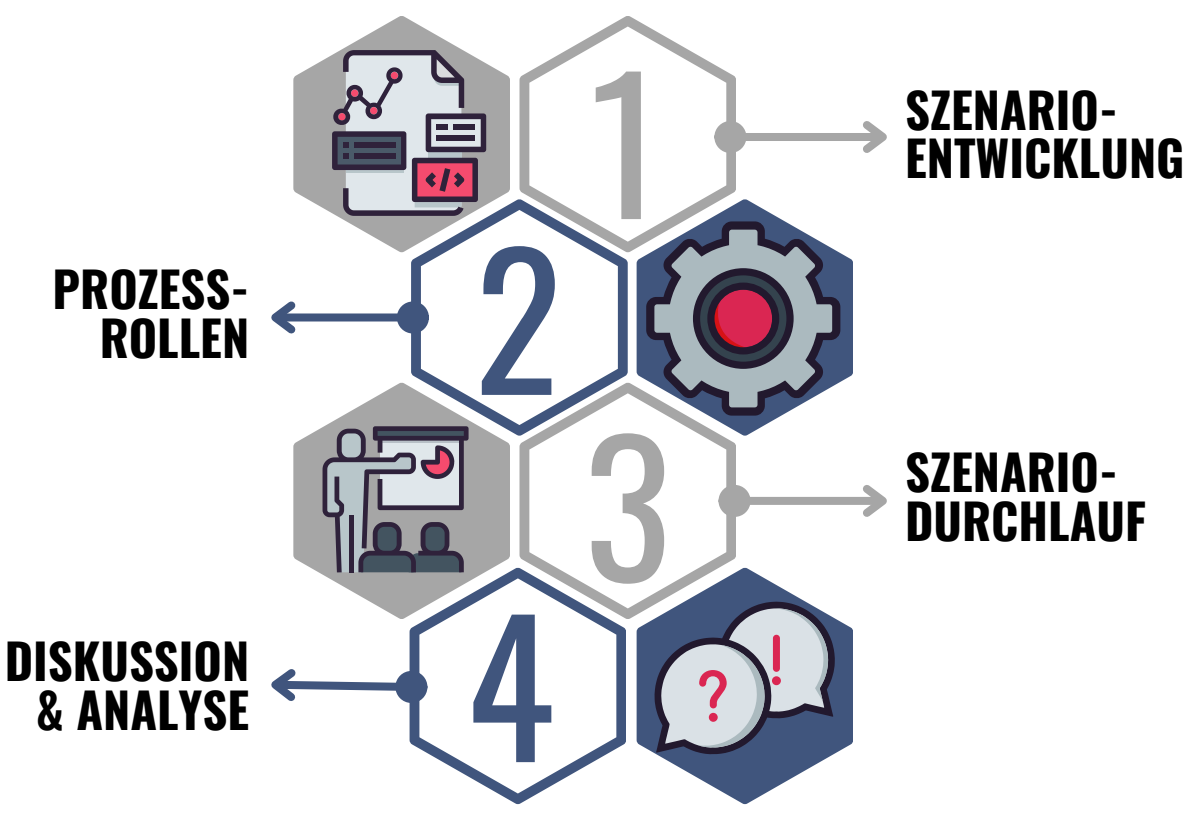
- Reaktion auf Sicherheitsvorfälle testen und verbessern
- Schwachstellen in Prozessen aufdecken

Anforderungen von Cybersecurity-Versicherungen:

- Nachweis angemessener Sicherheitsmaßnahmen
- Senkung von Versicherungsprämien

Ablauf einer Pen & Paper IT-Security Incident Übung

Der besondere Reiz von Pen & Paper IT-Security Incident Übungen liegt in ihrer realitätsnahen Simulation von Sicherheitsvorfällen. Hier ist, wie eine solche Übung ablaufen könnte:



1 **Szenarioentwicklung**: Ein Team von Sicherheitsexperten entwirft realistische Szenarien von Sicherheitsvorfällen, die auf die individuellen Risiken des Unternehmens zugeschnitten sind. Dies kann von einem Ransomware-Angriff bis zu einem Phishing-Versuch reichen.

2 **Prozess-Rollen:** Die Mitarbeiter werden in Teams aufgeteilt, um die Zusammenarbeit in stressigen IT-Security Incident Situationen zu simulieren. Jedes Team übernimmt eine bestimmte Rolle, sei es die IT-Abteilung, die Kommunikation oder das Management.

3 **Szenario-Durchlauf:** Die Teams arbeiten gemeinsam anhand der präsentierten Szenarien und entwickeln Strategien zur Bewältigung der angenommenen Bedrohungen. Die Interaktion erfolgt jedoch nicht in der technischen Umgebung, sondern in Form eines Rollenspieles.

4 **Diskussion und Analyse:** Nach Abschluss der Übung werden die Ergebnisse von den Sicherheitsexperten analysiert. Schwachstellen in den Prozessen, Kommunikationslücken und Verbesserungsmöglichkeiten werden identifiziert und Handlungsmaßnahmen abgeleitet.

Stärkung der Cyberresilienz durch gezielte Übungen

In einer Ära, in der Cyberangriffe unvermeidlich sind, ist die Vorbereitung auf diese Bedrohungen von entscheidender Bedeutung. Pen & Paper IT Security Incident Übungen bieten eine realistische und risikofreie Möglichkeit, die Reaktionsfähigkeit auf Sicherheitsvorfälle zu testen und zu verbessern. Die Anforderungen der ISO 27001 und von Cybersecurity-Versicherungen unterstreichen die Notwendigkeit solcher Übungen. Durch kontinuierliches Training werden nicht nur IT-Sicherheitsprozesse optimiert, sondern auch Mitarbeiter sensibilisiert, um in einer digital vernetzten Welt sicher agieren zu können.

"Durch regelmäßige Security-Prozessübungen werden Teams besser auf potenzielle Bedrohungen vorbereitet, was die Reaktionszeiten im Falle von Sicherheitsvorfällen erheblich verkürzen kann."

KONTAKTIEREN SIE UNS
Tilmann Sies
Lead Consultant/
Technology &
Organization
tilmann.sies@sepago.de

sepago. making people love it.