

# Schwachstellen erkennen und richtig reagieren.

#hackersnochance

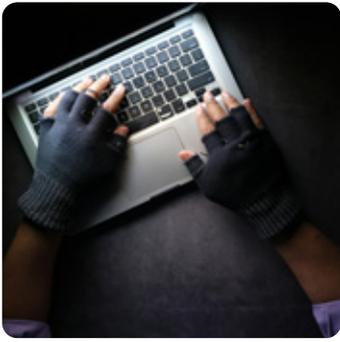
- **Was ist Schwachstellenmanagement?**  
Schwachstellenmanagement ist ein wichtiger Baustein, um die IT-Systeme in Organisationen gegen Cyberbedrohungen und Datenverlust zu schützen. Ziel ist es, Schwachstellen in den IT-Systemen zu erkennen, zu bewerten und zu schließen, bevor sie von möglichen Angreifern ausgenutzt werden können. Ein effektives Schwachstellenmanagement umfasst demnach die Erkennung von Schwachstellen (Schwachstellenscanner), eine Risikobewertung, die Beseitigung der Schwachstellen und regelmäßiges IT-Monitoring.

In Kooperation mit Enginsight bieten wir ein solches Schwachstellenmanagement an, bei dem wir anhand von Penetrationstests Sicherheitslücken in der IT aufdecken und – sollten Schwachstellen identifiziert werden – Handlungsempfehlungen aussprechen, wie Sie als IT-Verantwortliche die Lücken schließen und die Sicherheit des Unternehmens verbessern.

#### Schwachstellenscan

Welche Schwachstellen gibt es konkret in der IT-Infrastruktur Ihres Unternehmens oder im Unternehmen Ihres Kunden? Mit einem Schwachstellenscanner machen wir die betroffenen Assets sichtbar, damit sie umgehend gepatcht werden können. Ein Schwachstellenscanner ist ein IT-Security-Tool, das Schwachstellen in IT-Systemen erkennt und Netzwerke nach bekannten Sicherheitslücken durchsucht. Daraufhin erhalten Sie eine Übersicht über die potenziellen Risiken, die durch diese Lücken entstehen. Die automatisierte Bewertung des Schweregrads hilft bei der Priorisierung. So sind Sie immer über den Sicherheitszustand aller Assets informiert und wissen, wenn Handlungsbedarf besteht.

**Beheben der Schwachstellen:** Im Fall von Gefahren reagieren – je nach Art unserer Zusammenarbeit wir oder Sie – durch gezieltes Einspielen von Updates über mehrere Server und Clients hinweg. Das Tag-System erlaubt eine komfortable, plattformunabhängige Konfiguration auch in großen IT-Umgebungen.



- **Pentesting**

Penetrationstests (oder Pentests) sind Sicherheitsübungen, bei denen wir testen, ob Ihre aktuellen Schutzmaßnahmen einem Angriff wirklich standhalten würden. Wir „pentesten“ also quasi Ihre IT-Systeme aus dem Blickwinkel eines Angreifers. Sollten unsere simulierten Angriffe zur Sicherheitsprüfung zeigen, dass Handlungsbedarf besteht, erhalten Sie von uns einen Bericht mit Empfehlungen. So sehen Sie auf einen Blick, wie sicher Sie aufgestellt sind und an welchen Stellen der dringlichste Handlungsbedarf besteht. Bei regelmäßigen Audits haben Sie einen Vergleich, wie erfolgreich Ihre bisherigen Maßnahmen zur Härtung Ihrer IT-Systeme bereits waren.

Jetzt Schwachstellenscan beantragen und Schwachstellen im Unternehmen aufdecken. gesamten IT-Infrastruktur verschaffen.



Unser Sales Team berät Sie gerne zu unseren IT-Sicherheitslösungen +49 2203 202 07-80