# KONTINUIERLICHE UND AUTOMATISCHE ANGRIFFSSIMULATIONEN

**Ohne IT steht das Business still. Umso entscheidender also, Schwachstellen aufzudecken, bevor es Angreifer tun. Mit unserem Automatic Breach Simulation Service (ABS-Service) unterstützen wir dabei – und das völlig automatisiert durch Phishing-Kampagnen, auf Endpoints, durch Lateral Movement und Daten-Exfiltration. Der Vorteil gegenüber typischen Sicherheitstests ist die Simulation eines echten Angriffs mit inaktivierter Malware – ähnlich einer Impfung beim Arzt.**

## POTENZIELLE SCHWACHSTELLEN ERREICHEN REKORDWERT

Mit zunehmender Digitalisierung steigt die Anzahl der Sicherheitslücken. So verzeichnet das AV-TEST Institut mehr als 350.000 neue Malware und potenziell unerwünschte Anwendungen pro Tag – Tendenz steigend. Unternehmen müssen ihre Schutzmaßnahmen ausbauen, können das jedoch nur, wenn ihnen die Schwachstellen ihrer IT und potenzielle Angriffspunkte ihrer Mitarbeiter überhaupt bekannt sind.

In **60%** der Fälle sind Angreifer in der Lage, ein Unternehmen innerhalb von wenigen Minuten zu kompromittieren.*

Die meisten Security-Produkte **blockieren nur**

**46%** der E-Mails, die Ransomware enthalten.*

Wir unterstützen Sie kontinuierlich dabei, Sicherheitslücken aufzudecken und Ihre Mitarbeiter zu sensibilisieren. Wir setzen auf ein ähnliches Konzept, wie Ihr Arzt bei Impfungen – nur dass unsere Viren und Malware inaktiv sind. Ihre Systeme und Mitarbeiter werden auf Herz und Nieren geprüft und trainiert. Beispielweise verwenden wir ungefährliche Phishing-Mails, mit denen das Mail Gateway getestet und die Empfänger-Awareness geschärft wird.

Unser Service simuliert einen Angriff auf Endpunkte und zeichnet die Schwachstellen auf, die ein solcher Angriff ausnutzen würde. Somit sehen Sie, welche Auswirkungen und Ausmaße ein solcher Angriff in der Realität auf Ihr Unternehmen hätte. Basierend auf diesen Erkenntnissen formulieren wir effektive Handlungsempfehlungen, mit denen Sie die Schwachstellen schließen können. Durch den ABS-Service erhalten Sie zudem Aussagen über den aktuellen Zustand Ihrer IT-Sicherheit und die Wirksamkeit präventiver Maßnahmen.

## MASSGESCHNEIDERTER SERVICE

Ob Ihre Systeme, Infrastrukturen oder Mitarbeiter – Dank unseres modularen Services können Sie selbst entscheiden, welchen Bereich Sie genauer unter die Lupe nehmen möchten. Wir analysieren folgende Angriffsvektoren:

- **Web Gateway:** In dieser Überprüfung wird getestet, inwieweit bösartige Webseiten mit einem Browser über das HTTP(S)-Protokoll aufgerufen werden können und diese durch das Gateway geblockt werden.
- **Web Applikation Firewall (WAF):** Wir analysieren die Top 10 Schwachstellen des Open Web Application Security Projects (OWASP), wie zum Beispiel SQL-Injektion, Command Injection oder Cross-Site-Scripting.
- **Phishing-Kampagne:** Wir überprüfen, wie sicherheitsbewusst Ihre Mitarbeiter mit E- Mails umgehen und testen das Mail-Gateway auf sicherheitskritische Anhänge und Hyperlinks.
- **Endpoint-Kampagne:** Hier erhalten Sie ein umfassendes transparentes Bild zur Sicherheitslage der Endpoints in Ihrem Unternehmen.
- **Lateral Movement Assessment:** Wir identifizieren das Risiko Ihrer IT-Landschaft, wenn ein Endpunkt gefährdet wurde sowie das davon ausgehende Gefährdungspotenzial auf weitere Endpunkte.
- **Daten-Exfiltration:** Wir prüfen, ob kritische Informationen über Netzwerkprotokolle über die Organisationsgrenzen hinweg abfließen können.

Gemeinsam ermitteln wir Ihren individuellen Bedarf und den dazu passenden Umfang der Maßnahmen.

## GEFAHR ERKANNT, GEFAHR GEBANNT. IMMER WIEDER.

Greifen Sie regelmäßig auf den ABS-Service zurück, profitieren Sie von einer kontinuierlichen Optimierung Ihrer IT-Sicherheit. Basierend auf der abschließenden Übersicht aller gefundenen potenziellen Schwachstellen erhalten Sie eine Bewertung und Priorisierung dieser. So haben Sie volle Transparenz über potenzielle Gefahren und mögliche Auswirkungen auf das Unternehmen. Auf Wunsch erarbeiten wir anschließend gemeinsam ein umfassend abgestimmtes Vorgehen, um Ihre IT-Landschaft zu schützen.

Computacenter

**Computacenter AG & Co. oHG**
Computacenter Park 1, 50170 Kerpen

**computacenter.de**
+49 (0)2273 5970

*Quelle: Cymulate.com