

Frequently Asked Questions (FAQ)

Phishing Simulation

IT-Seal GmbH
Tel: 06151/4938989

Inhalt

Inhalt	1
Cyber-Attacken: Phishing	2
Was ist Phishing?	2
Juristisch	2
Sind solche Simulationen zulässig?	2
Darf ich also meine Mitarbeiter überwachen?	2
Dürfen Mitarbeiterdaten übertragen werden?	2
Datenschutz	2
Welche Daten werden übertragen?	2
Sammelt IT-Seal darüber hinaus noch weitere Daten?	3
Wo befinden sich die datenverarbeitenden Server?	3
Wie geht IT-Seal mit IT-Sicherheit um?	3
Hat IT-Seal einen Datenschutzbeauftragten eingesetzt?	3
Geht die Datenverarbeitung bei IT-Seal mit der DSGVO konform?	3

Cyber-Attacken: Phishing

Cyber-Attacken bilden heute ein großes industrielles, wirtschaftliches und soziales Problem. Studien zeigen, dass über 90% der gezielten Cyberangriffe und 95% der Spionageangriffe Phishing oder personalisierte Spear-Phishing-E-Mails beinhalten¹ und insgesamt durchschnittlich 10% der Phishing-Angriffe erfolgreich sind.²

Was ist Phishing?

Phishing bezeichnet gefälschte Nachrichten, mit denen ein Angreifer versucht an die Systeme oder Daten seines Opfers zu kommen. Dazu sendet der Angreifer typischerweise eine E-Mail mit gefälschtem Absender, in der er eine schadhafte Datei oder einen gefälschten Link anhängt. Beim Klick auf einen solchen, kann es bereits zu spät sein: Eine vorbereitete Website kann bei einem Besuch bereits ein System infizieren.

IT-Seal simuliert diese Art von Angriffe auf Mitarbeiter. Auf diese Weise machen Mitarbeiter realitätsnahe Erfahrungen, werden trainiert und getestet.

Juristisch

Sind solche Simulationen zulässig?

Social Engineering Simulationen sind generell nur zulässig, wenn Sie verhältnismäßig sind. Daher müssen verschiedene Maßnahmen wie z.B. die Anonymisierung der Ergebnisse ergriffen werden.

IT-Seal ergreift alle relevanten Schritte vorab und unterstützt Sie bei der internen Kommunikation soweit nötig.

Darf ich also meine Mitarbeiter überwachen?

Nein. Um den Schutz des einzelnen Mitarbeiters zu gewährleisten, sind die Ergebnisse nur auf Gruppenbasis einsehbar. Dazu verwenden wir die von Ihnen vorab definierten Mitarbeitergruppen mit einer Mindestgröße von 15 Teilnehmern.

Dürfen Mitarbeiterdaten übertragen werden?

Die Übermittlung und Verwendung der Daten sind gestattet, wenn ein berechtigtes Arbeitgeberinteresse vorliegt und schutzwürdige Interessen des betroffenen Arbeitnehmers nicht entgegenstehen. Daher sollte der Arbeitgeber keine intern bekannten Daten übermitteln, die ein „echter“ Angreifer nicht ohne Weiteres erfahren könnte. Zudem muss eine Vereinbarung zur Auftragsdatenverarbeitung oder zur Funktionsübertragung geschlossen werden.

Datenschutz

Welche Daten werden übertragen?

Im Einklang mit den gesetzlichen Bestimmungen wird im Rahmen der anfänglichen Zusammenarbeit die E-Mail-Adresse von ausgewählten Mitarbeitern an IT-Seal übertragen.

¹ <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf>

² <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/>

Sammelt IT-Seal darüber hinaus noch weitere Daten?

Im Rahmen der anfänglichen Zusammenarbeit werden lediglich Daten zur Nutzerreaktion gesammelt. Dazu zählen wir, ob Mitarbeiter auf einen gefälschten Link geklickt haben, oder ob Nutzerdaten auf einer präparierten Website eingegeben wurden – die Inhalte dieser Dateneingabe werden nicht übertragen. Diese Daten werden, wie zuvor beschrieben, abstrahiert (pseudonymisiert) gespeichert. Wobei die Zuordnung der Pseudonyme nach Abschluss des Tests gelöscht wird.

Wo befinden sich die datenverarbeitenden Server?

IT-Seal nutzt ein Rechenzentrum in Frankfurt am Main mit höchsten Sicherheitsanforderungen.

Wie geht IT-Seal mit IT-Sicherheit um?

Wie aktuelle Angriffe immer wieder verdeutlichen, ist leider niemand unhackbar – auch wir nicht. Als IT-Security Spezialist implementiert IT-Seal jedoch aktuellste Sicherheitsmechanismen und bereitet sich auf eventuelle Sicherheitsverstöße intensiv vor (für konkrete technische und organisatorische Maßnahmen legen wir Ihnen gerne eine vorbereitete Vereinbarung zur Funktionsübertragung vor). So sind auch unsere Datenbankstrukturen und Prozesse von Grund auf so angelegt, dass personenbezogene Daten immer gesondert abgelegt werden (Security by Design). Zudem werden standardmäßig jegliche personenbezogenen Daten nach Abschluss der jeweiligen Simulation gelöscht.

Hat IT-Seal einen Datenschutzbeauftragten eingesetzt?

Ja. Die Kontaktdaten werden auf Anfrage gerne weitergereicht.

Geht die Datenverarbeitung bei IT-Seal mit der DSGVO konform?

Ja. Unsere Prozesse und Normen zum Datenschutz gehen zu weiten Teilen über die Anforderungen der bisherigen gesetzlichen Anforderungen hinaus (z.B. das Löschen der personenbezogenen Daten, Datenschutzfolgenabschätzung) und genügen den Anforderungen der DSGVO.

Für weitere Fragen kontaktieren Sie uns gerne:



David Kelm
Geschäftsführer der IT-Seal GmbH

Hilpertstr. 31
64295 Darmstadt
+49 (0) 6151/4938989
www.it-seal.de



IT-SEAL