KERKAPORTA
</ IT SECURITY GMBH>

Portfolio

Kerkaporta bietet Ihnen ein maßgeschneidertes Sicherheitspaket, das Ihre Anforderungen im Bereich IT Security umfassend abgedeckt.

</ Web Application Audit >

Potenzielle Angreifer nutzen Sicherheitslücken um an vertrauliche Daten in Ihrem Unternehmen wie Benutzernamen, Passwörter, Inhalte von E-Mails oder diverse Dokumente zu gelangen. Auch der Zugriff auf Server oder benachbarte Systeme durch Fremde kann neben Imageverlusten auch zu einem finanziellen Schaden für den Betreiber als auch für Kunden führen.

Aktuelle Studien belegen, dass mindestens 70% der weltweiten erreichbaren Webpräsenzen Sicherheitslücken aufweisen.

Um Ihre Webpräsenz umfassend zu schützen, bietet Kerkaporta Web Application Security Audits für Ihre eingesetzten Webapplikationen:

- Content Management Systeme,
- Intranet Seiten
- Webshops,
- Online Redaktionssysteme
- Webblogs
- Eigene Entwicklungen

Gerade bei eigenen Entwicklungen unterlaufen leicht sicherheitsrelevante Fehler in der Konzeption, Implementierung oder Betrieb. Da Webanwendungen nicht immer vor der Inbetriebnahme speziellen Sicherheitstests unterzogen werden, enthalten viele Schwachstellen wie Cross-Site-Scripting (XSS), SQL-Injection oder Cross-Site-Request-Forgery. Auch Logikfehler, welche z.B. Inhalte unberechtigten Benutzern zugänglich machen sind oft Bestandteil solcher Software.

Mit Erfahrung, Know-How und unter der Einhaltung von hohen Qualitätsstandards prüfen wir Ihre Webanwendungen. Die Audits werden nach OWASP-Richtlinien durchgeführt und entsprechen somit den aktuellen Standards und den höchsten Qualitätsanforderungen.

</ Client Audit >

Beim Client Audit stehen vor allem jene Arbeitsmittel im Fokus, mit denen Ihre Mitarbeiter tagtäglich arbeiten: Workstation, Notebook oder Smartphone. Erfahren Sie im Detail welche Berechtigungen Ihre Mitarbeiter haben und wie weit sie in die Systeme Ihres Unternehmens Zugriff haben. Die Security-Einstellungen, die Verschlüsselung von Festplatten und die Aktualität Ihrer Systeme werden ebenfalls einer umfassenden Analyse unterzogen. Nach einem Client Audit haben Sie Gewissheit, wer und in welchem Ausmaß in Ihre Systemen eingegriffen werden kann. Gegebenenfalls können danach Sicherheits-Maßnahmen abgeleitet werden und Berechtigungen verändert werden. Erhalten Sie auch in diesem Prozess Unterstützung von Kerkaporta.

</ Server Audit >

Neben Client Audits können Sie auch Ihren Server einem Audit unterziehen. Bei diesen Überprüfungen geben wir Ihnen Aufschluss darüber, wie der Server konfiguriert ist, wie z.B. Einstellungen in der Active Directory aussehen und ob alle Security Patches installiert sind.

</ Network Security >

Wie gut kennen Sie Ihr Netzwerk?
Netzwerksicherheit geht über die sichere Vernetzung innerhalb des Unternehmens hinaus: Der Schutz von Netzwerkzugängen und Netzwerkverbindungen mit externen und mobilen Geräten sowie mit Cloud-Services und anderen Internetdiensten hat ebenfalls einen hohen Stellenwert. Die Vernetzung bringt viele Vorteile mit sich, doch auch die Risiken wie zum Beispiel Lauschangriffe oder Manipulation von übertragenen Daten steigen an. Deshalb sind die Überwachung von Netzwerkinfrastrukturen sowie der Schutz gegen unerlaubte Zugriffe unumgänglich um das höchste Maß an Sicherheit erhalten.

Erfahren Sie mehr rund um Ihr Netzwerk und dessen Zusammensetzung. Kerkaporta vermittelt Ihnen ein Verständnis für Angriffsmöglichkeiten von Hackern auf Ihr Netzwerk oder welche Schäden ein unbekanntes Gerät in Ihrem Netzwerk verursachen kann. Mit unserer fachlichen Expertise erhalten Sie umfassenden Schutz für Ihr Netzwerk.

</ Training >

Um die Sicherheit in Ihrem Unternehmen zu gewährleisten, ist nicht nur eine gut geschützte IT-Infrastruktur erforderlich, sondern auch ein grundlegendes Verständnis der IT-Sicherheit bei Ihren Mitarbeitern. Gerade in der alltäglichen Routine im Umgang mit IT-Systemen sehen Cyberkriminelle oft einen potenziellen Angriffspunkt. Der „Faktor Mensch“ rückt daher in den Mittelpunkt krimineller Angriffe. Mit Hilfe eines Awareness Trainings lernen Ihre Mitarbeiter potenzielle Gefahren zu erkennen und riskantes oder fehlerhaftes Verhalten im beruflichen Alltag zu vermeiden. Stärken Sie das Bewusstsein Ihre Mitarbeiter für das Thema IT Sicherheit und geben Sie ihnen das notwendige Know-How um Angriffe rechtzeitig zu erkennen und angemessen darauf zu reagieren.

Inhalte unserer Awareness-Trainings:

- Versetzen Sie sich in einen Hacker! Welchen Schaden kann ein Hacker anrichten und wie geht er dabei vor
- Sicherheit im Umgang mit E-Mails: Phising-Mails erkennen
- Sicherheit mit Passwörtern
- Erkennen von gefälschten Links in E-Mails oder Dokumenten
- Bedrohung durch Computerviren: Wie verhalten Sie sich bei einem Virenbefall und was können Sie in dieser Situation tun

</ Secure Coding >

Fehler, Bugs oder Logikfehler sind häufige Ursachen für Softwareschwachstellen, die eine potenzielle Gefahr für Cyberangriffe darstellen. Sicherheitskritische Fehler werden oft erst im Zuge von Penetrationstests oder erfolgreichen Hacking-Angriffen erkannt. Die Behebung dieser Fehler kann mit hohen Kosten verbunden sein. Um eine sichere Software zu entwickeln ist Secure Coding daher eine notwendige Voraussetzung, um Sicherheitslücken gar nicht erst entstehen zu lassen.

Für die Kerkaporta IT Security GmbH steht bei der Programmierung von Webanwendungen die Sicherheit im Fokus. Der Sicherheitsaspekt fließt bereits in die Planung der Programmierung mit ein. Profitieren Sie von maßgeschneiderten, sicherheitsorientierten Anwendungen, die Ihnen User-Freundlichkeit und eine einfache Handhabung bieten.