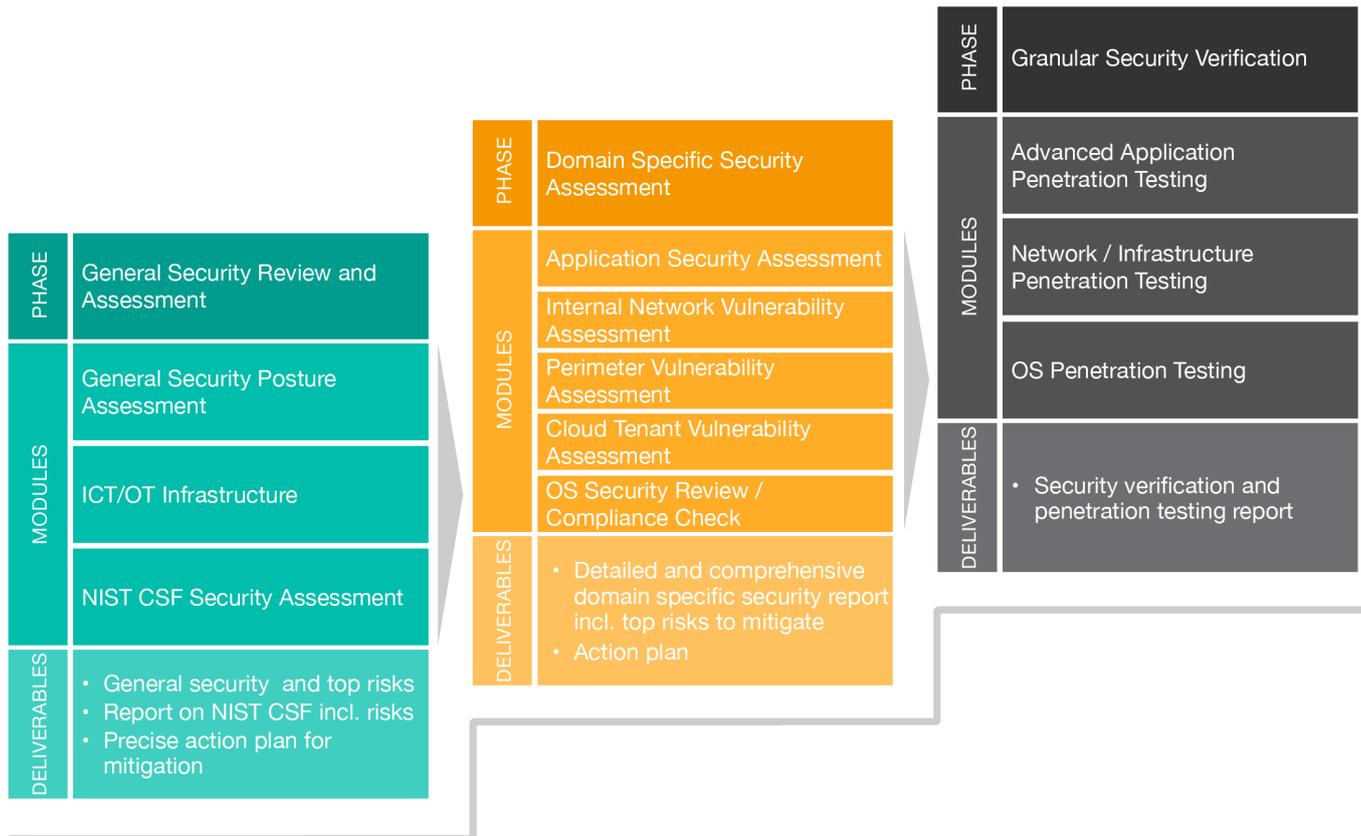


SECURITY ASSESSMENTS

Unternehmen wissen oft nicht genau, wie es um die Sicherheit in ihrer IT-Infrastruktur steht. Sind die Informationssysteme aktualisiert und gegen Angriffe und Viren geschützt? Ist das Sicherheitskonzept vollständig und wird dies auch laufend überprüft? Noch viel schwieriger ist es oft zu beantworten, wo das Unternehmen zuerst ansetzen soll, um das Risiko für Cyber-Angriffe zu verringern. Mit den auf Ihre Bedürfnisse zugeschnittenen Security Assessments zeigen wir Ihnen die Schwachstellen und Risiken in Ihrem Unternehmen auf und unterstützen Sie bei der Behebung dieser.



Viele Unternehmen entscheiden sich als erstes für ein Penetration Test um die Sicherheit ihrer Infrastruktur zu überprüfen. Penetration Tests sind jedoch oft nicht eine effiziente Methode, um einen guten Überblick der Risiken und Schwachstellen zu erhalten. Zwar liegt nach einem Penetration Test ein Schwachstellen-Report vor, die grundlegenden Ursachen, wieso Schwachstellen entstanden sind, werden jedoch nicht behoben. Des Weiteren besitzt jedes Unternehmen und jede IT Infrastruktur unterschiedliche Komponenten, Anforderungen und Risiken, eine einheitliche Lösung für jedes Unternehmen ist also nicht möglich.

Clue setzt deshalb auf einen dreistufigen Ansatz, welcher mit einer holistischen Herangehensweise alle für den Kunden nötigen Betrachtungsweisen der Cyber-Sicherheit mit einbezieht. Unsere langjährigen Erfahrungen zeigen, dass unser Vorgehen nicht nur nachhaltiger ist für unsere Kunden, sondern auch kostengünstiger als andere Angebote am Markt.

Wir bieten Ihnen modulare und auf Ihre Bedürfnisse zugeschnittene Security Assessments an, welche Ihnen helfen, Schwachstellen zu identifizieren, die Risiken einzuschätzen und vernünftige Gegenmassnahmen umzusetzen. Dabei berücksichtigen wir bereits von Kunden eingesetzte Methoden und Technologien zum Security Monitoring wie SOC Services, SIEM, Vulnerability Management und regelmässige Audits und passen unser Vorgehen daran an.

So profitieren Unternehmen, welche ihr Sicherheits-Niveau einschätzen möchten, ohne bereits einen oder mehrere dieser Services einzusetzen genauso wie Unternehmen, die gezielt Systeme, Web-Applikationen, IoT oder Incident Response Teams testen wollen. Unsere Assessments reichen von einer Bewertung der Security Maturität auf organisatorischer Ebene über die Erkennung und Bewertung von Schwachstellen bis zum allumfassenden Penetration Test.

ANGEBOTENE MODULE

GENERAL SECURITY POSTURE ASSESSMENT

Um einschätzen zu können, welche Schritte bereits in Richtung Cyber-Sicherheit unternommen wurden, kann einleitend ein Security Posture Assessment durchgeführt werden. Dies schafft einen Überblick darüber, welche Massnahmen bereits ergriffen wurden und dient als Grundstein für weiterführende Gespräche.

ICT / OT INFRASTRUCTURE DIAGRAMMING

Um den Kontext der zu untersuchenden Infrastruktur zu verstehen, wird in gemeinsamen Diagramming-Workshops der zu betrachtende Scope visualisiert.

NIST CSF SECURITY ASSESSMENT

Der Kern unseres Security Assessments auf Stufe 1 bildet der international anerkannte und weit verbreitete Standard NIST CSF (National Institute of Standards and Technology – Cyber Security Framework). Diesen reichern wir bedarfsgerecht mit unserem Wissen und den Bedürfnissen des Assessment-Scope an. Die Verwendung des Standards erlaubt eine holistische und stufenweise Betrachtung des Themenkomplexes auf Ebenen wie Management, Prozesse, Schutzmechanismen, Awareness, Erkennungsfähigkeiten und Reaktionsfähigkeiten. Die dadurch gewonnen Ergebnisse erlauben einen massgeschneiderten und priorisierten Massnahmenplan welcher zu einer Beleuchtung aller wichtigen Themen zur Verbesserung des Schutzniveaus führt. Durch die weite Verbreitung des NIST CSF unterstützen diverse andere Management Standards seine Terminologien und können seine Ergebnisse verknüpfen. Somit können die Ergebnisse aus dem Assessment bei Bedarf in diversen anderen Standards weiterverwendet werden.

APPLICATION SECURITY ASSESSMENT

In einem Application Security Assessment analysieren wir die Sicherheit einer Applikation über verschiedene Methodiken, um dem Kunden ein Bild über den Stand der Sicherheit dieser zu geben und ihm Verbesserungsmöglichkeiten aufzuzeigen. Dabei begleitet Clue Kunden auch dabei, Massnahmen einzuführen, um die Sicherheit von Software-Eigenentwicklungen nachhaltig zu steigern. Für genauere Informationen wird unser dediziertes Application Security Consulting Fact Sheet empfohlen.

VULNERABILITY ASSESSMENTS UND OS SECURITY REVIEWS / COMPLIANCE CHECKS

Bei Vulnerability Assessments und OS Security Reviews / Compliance Checks überprüft Clue Ihre im Scope befindliche Infrastruktur oder deren Komponenten auf Schwachstellen in der Software und Hardware. Wir identifizieren potenzielle Hintertüren, die durch unsicher konfigurierte Systeme entstehen können, und führen Audits zu deren Konfiguration durch. Unser Team steht Ihnen bei der Erkennung, Analyse und Bewertung von Schwachstellen zur Seite und unterstützt Sie dabei, diese effizient und effektiv zu beheben. Angesichts der erfolgreichen Angriffe von Malware auf verschiedene IT-Infrastrukturen von Unternehmen ist es entscheidend, dass jedes Unternehmen proaktiv Schwachstellen und Fehler in der Konfiguration angeht. Viele Angriffe basieren auf Schwachstellen und Advisories, die bereits seit einiger Zeit öffentlich bekannt sind.

PENETRATION TESTING

Ein Clue Penetration Test ist ein realitätsnaher Angriff auf Ihre IT-Infrastruktur. Dabei werden reale Bedingungen nachgestellt und ohne Zutun der internen Business Units Mensch und Maschine wie bei einem Hacker-Angriff getestet. Im Gegensatz zu Vulnerability Assessments verlässt Clue sich nicht nur auf vollautomatisierte Tests. Schwachstellen und Konfigurationen werden durch Exploits und offensives Vorgehen validiert. Unser Ziel ist es, alle Sicherheitslücken und Schwachstellen aufzudecken, anstatt nur «einen» Weg in das Unternehmensnetzwerk zu finden und andere mögliche Schwachstellen zu ignorieren. Somit werden alle involvierten Angriffsvektoren in Laufzeit über ein strukturiertes Verfahren manuell nach Schwachstellen hin untersucht und ausgenutzt.

NÄCHSTE SCHRITTE

Sie müssen wissen, wie es heute um die IT-Security in Ihrem Unternehmen steht? Sie vermissen ein aktualisiertes Inventar aller IT-Komponenten und deren Kommunikationswege? Sie brauchen Expertenwissen für ein Migrationsprojekt oder das bevorstehende Audit? Sprechen Sie uns auf ein Security Assessment und Penetration Testing an. Gerne beraten wir Sie und zeigen Ihnen eine auf Ihre Umgebung angepasste und zielführende Umsetzung auf.

