Antares-NetlogiX

VULNERABILITY MANAGEMENT SERVICE

Steigen Sie mit uns in die Welt der Cybersecurity ein! **Unsere Experten identifizieren für Sie mögliche Schwachstellen** und validieren die Ergebnisse. Mit unserem Vulnerability Management Service sichern Sie Ihr Unternehmen gegen komplexe Sicherheitsbedrohungen, ohne selbst großen Aufwand betreiben zu müssen.

MEHR ALS STANDARD-SOFTWARE

Tools & Know-how für höchste Sicherheit

Die Antares-Experten führen zuerst eine **initiale Überprüfung** durch, die Ihnen einen Überblick über die aktuelle Sicherheitslage verschafft. Wir stellen die Ergebnisse in Form eines ausführlichen Reports (PDF-Datei) für Sie bereit. Dieser ist auch die Grundlage für alle weitergehenden Scans:

Mit der **regelmäßigen Folgeprüfung** testen wir je nach Kundenwunsch wöchentlich, monatlich oder quartalsweise alle extern erreichbaren Systeme auf Schwachstellen bzgl. Überwindbarkeit bzw. jegliche Art von Manipulation.

Über **Delta-Reports** behalten Sie den Überblick über die Änderungen der Sicherheits-bedrohungen. Unser **ANTARES RED TEAM** hat die Erfahrung, wenn es um das Aufspüren von Schwachstellen geht.

Verwalten Sie den Lebenszyklus Ihrer Schwach-stellen ab sofort ganz bequem in unserem Vulnerability Lifecycle Manager.

Wir bieten Ihnen nicht nur Schwachstellen-Scans und fundierte Auswertungen, sondern auch die Behebung ebendieser: **Managed Patching.**

WIR HABEN DAS **KNOW-HOW**

Managed Vulnerability Scans

Antares-Red-Team-Leiter Stefan Winkler und weitere vier Pentester und Auditoren haben viel zu tun: mehr als 50 Penetrationstests pro Jahr sowie Planung und Umsetzung vieler Security-Projekte.

Das Team beschäftigt sich permanent mit den aktuellen Security-Ereignissen, da ständig Systeme kontrolliert oder diese „gehackt" werden müssen. Neben jahrelanger Erfahrung und dem Know-how aus vielen Audits und Penetrationstests fließen auch aktuelle Erkenntnisse in die Reports und Verbesserungsvorschläge ein. Ein äußerst hilfreiches Tool für die Verwaltung von Schwachstellen ist unser selbst entwickelter **Vulnerability Lifecycle Manager (VLM)**.

ANTARES
RED TEAM

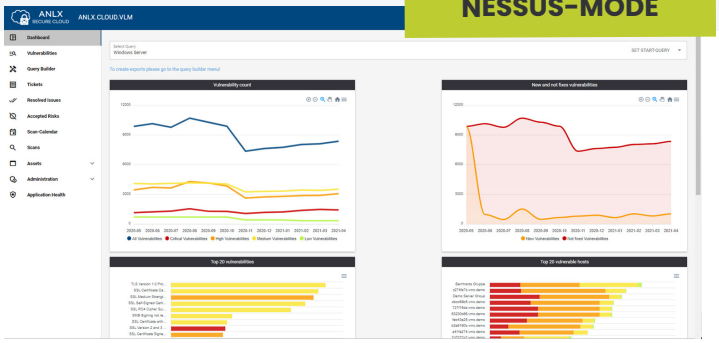
IHR **EXPERTE**

SOC-Leiter BERNHARD HOCHAUER über den VLM

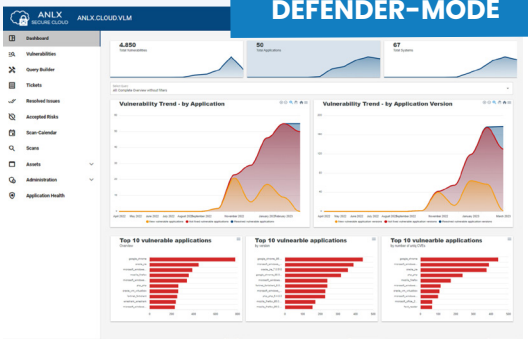
„Der VLM sammelt sämtliche Schwachstellen aus den einzelnen Scans in einem **zentralen Dashboard** und gibt somit eine klare Übersicht über den Zustand der Unternehmensumgebung - sowohl für die Techniker als auch für das Management.

Ein **Ticketing System** in der Plattform sorgt für eine übersichtliche Abarbeitung der offenen Vulnerabilities – geschlossene Tickets werden automatisch auf Reopened gesetzt, falls die Schwachstelle wieder auftritt. Den VLM gibt es für **Tenable Nessus** oder **Microsoft Defender**."

NESSUS-MODE



DEFENDER-MODE



SICHERHEIT UND **DATENSCHUTZ**

Wir bieten Ihnen ein Höchstmaß an Sicherheit.

RECHTSVORGABEN

Österreichisches und EU-Recht

ISO 27018 Data Protection for Cloud Services

Der Betrieb unserer Services erfolgt **ausschließlich in österreichischen Rechenzentren** und ist damit nur österreichischem und EU-Recht unterworfen. Unsere Mitarbeiter werden regelmäßigen **Sicherheitsprüfungen** unterzogen, haben **Vertraulichkeitserklärungen** zu unterfertigen und werden jährlich in die entsprechenden **Sicherheitsstandards** unterwiesen (PCI DSS, Grundschutzhandbuch, etc.).

Von Antares-NetlogiX werden **keine Daten** (die über das administrativ Unumgängliche hinausgehen, wie z. B.: Lizenzdaten) an inländische oder ausländische Behörden bzw. Unternehmen **weitergegeben.**

ADMINISTRATION & SYSTEMWARTUNG

mit Erfahrung und Sicherheit

ISO 27001 Information Security Management Services

Die Administration unserer Services erfolgt ausnahmslos über **personenbezogene Accounts** und - sofern technisch realisierbar - über eine **Zwei-Faktor-Authentifizierung.** Die Zugriffe werden revisionssicher archiviert.

Alle **Administratoren verfügen über jahrelange Erfahrung** im Betrieb von Hochsicherheits- und Hochverfügbarkeitslösungen im Bankenumfeld.

Alle Systeme werden durch unsere Spezialisten **regelmäßig auf Schwachstellen** überprüft und - falls notwendig - entsprechende **Anpassungen** bzw. **System-Updates** umgehend durchgeführt.