CLAUSOHM. Software++ Automation

Clausohm-Software GmbH
Neubrandenburger Str. 46
D - 17039 Neverin
Tel : +49 39 608 26 90 00

www.clausohm.de

Clausohm-Software GmbH ■ Neubrandenburger Str. 46 ■ D - 17039 Neverin

Vorstellung
Konzept

Sicherheitsüberprüfung

Cyber Security by Clausohm

Verantwortlich:	Stefan Otto, Clausohm-Software GmbH Andreas Thiel, Clausohm-Software GmbH
Version:	1.0
Datum:	03.06.2024

CLAUSOHM. Software++ Automation

Clausohm-Software GmbH
Neubrandenburger Str. 46
D - 17039 Neverin
Tel : +49 39 608 26 90 00

www.clausohm.de

Inhalt

CLAUSOHM. Software++ Automation

Clausohm-Software GmbH
Neubrandenburger Str. 46
D - 17039 Neverin
Tel : +49 39 608 26 90 00

www.clausohm.de

1. Unternehmensvorstellung

Die Clausohm-Software GmbH ist ein Familienunternehmen, das 1990 in Neverin gegründet wurde und sich auf komplexe IT-Lösungen für Automatisierungsprozesse sowie auf webbasierte Plattformen spezialisiert hat. Unsere Kunden sind renommierte Großunternehmen, die international tätig sind.

Als Spezialist für Softwareentwicklung sind wir der ideale Partner bei Ihrer digitalen Transformation. Als unabhängiger Dienstleister erarbeiten wir maßgeschneiderte Lösungen von der IT-Strategie bis zur fertigen Software, die für schlanke und reibungslose Arbeitsabläufe sorgen, so dass Sie sich voll und ganz auf Ihr Kerngeschäft konzentrieren können.

Unser Team von mehr als 85 Ingenieuren aus den Bereichen IT und Automation, darunter IT-Projektleiter, Architekten, Entwickler, Tester, Qualitätsmanager, Cyber Security Analysten, Konstrukteure, Elektriker und SPS-Programmierer, stehen für jahrelange Praxiserfahrung, Technologiekompetenz und zertifizierte Qualität.

Wir legen Wert auf eine nachhaltige Wertschöpfung, vertrauensvolle Kundenbeziehungen und nehmen unsere soziale Verantwortung gegenüber unseren Mitarbeitern ernst. Für uns hat Gesundheit einen hohen Stellenwert. Ob gesunde Ernährung, Bewegung oder Coaching, wir fördern das Wohlergehen unserer Beschäftigten.

Neben der Zertifizierung nach ISO9001:2015 als Management-System sind wir mit TISAX LV2 im Bereich Informationssicherheit zertifiziert. Des Weiteren weisen wir für jedes Teammitglied Personenzertifizierungen nach. Diese umfassen den Cyber Security Practitioner vom Berufsverband ISACA, den IT-Grundschutz-Praktiker (BSI) sowie den CompTIA Security+ und CompTIAPentest+.

Neben den Schwachstellenanalysen und Penetrationstests sind Quellcode-Analysen, Dynamische Analysen des Netzwerkverkehrs sowie Beratungsdienstleistungen und Unterstützungen bei Sensibilisierungsmaßnahmen ständige Leistungen durch uns.

Clausohm-Software GmbH
Neubrandenburger Str. 46
D - 17039 Neverin
Tel : +49 39 608 26 90 00

www.clausohm.de

1.1 Unternehmensdaten

Unternehmen	- Unternehmensform GmbH - 85 Mitarbeiter, zusätzlich externe Mitarbeiter - Gründung 1990 - 3 Standorte (Neverin, Aachen und Berlin) - Geschäftsführung: Katharina, Carina und Heiner Clausohm

Zertifizierungen	- Qualitätsmanagementsystem nach **ISO 9001:2015**
	- Informationssicherheitsmanagementsystem (ISMS) nach **TISAX LV2**
	  o Organisation der Informationssicherheit
	  o Leitlinie und Richtlinien zur Informationssicherheit
	  o Strukturierung der IT-Systeme und Netzwerke
	- Datenschutzmanagementsystem

1.2 Geschäftsbereiche

Geschäfts-bereiche	- **Softwareentwicklung**
	  o Entwicklungsleistungen im Front- und Backend in den Bereichen E-Commerce Plattformen, Shoppingsystemen, Sales-Anwendungen über Web-Applikationen
	- **Automation**
	  o Schaltschrankbau, Elektrokonstruktionen & SPS-Programmierung
	  o Softwareentwicklung des unternehmenseigenen Produktionsinformationssystem CIRCLE
	- **Cyber Security**
	  o Externe Sicherheitsüberprüfungen von Online-Plattformen und IT-Infrastrukturen (White Hat Hacking)
	  o Mitarbeiterschulungen für Cyber Awareness

Clausohm-Software GmbH
Neubrandenburger Str. 46
D - 17039 Neverin
Tel : +49 39 608 26 90 00

www.clausohm.de

1.3 Referenzen

Insgesamt haben wir bereits eine Vielzahl an Schwachstellenanalysen von Online-Plattformen, Sicherheitsüberprüfungen der IT-Infrastruktur und Awarenesskampagnen mit Schulungen von MitarbeiterInnen durchgeführt.

Die folgende Auswahl verfügbarer Referenzen können wir angeben:

- Sicherheitsüberprüfung Amt Neverin,
- Kommunaler IT-Aufgabenträger / Stadt Neubrandenburg,
- Kommunaler IT-Aufgabenträger / Landkreis Vorpommern-Greifswald,
- Hochschule Neubrandenburg
- und die Stadtwerke Neubrandenburg können wir angeben:

Amt Neverin	- Sicherheitsüberprüfung IT-Infrastruktur - Sicherheitsüberprüfung vor Ort - Durchführung von Phishing Mailkampagnen
Ansprechpartner	- Alexander Diekow (Leitender Verwaltungsbeamter)
Umfang	- Schwachstellenanalysen von (Sub-) Domains und IP-Adressen - Versand Phishing E-Mails an die Mitarbeiter mit Auswertung und Ergebnispräsentation - vor Ort Begehungen zur Prüfung auf IT-Schwachstellen und Mitarbeiterverhalten
Umsetzung	- Durchführung vorbereitender Maßnahmen wie Kickoffs, Klärung Ansprechpartner und Eskalationswege, Bestimmung Ziele und Ablauf - Informationsbeschaffung durch Portscans, Schwachstellenscans und Webanwendungsscans mit den Standards nach BSI und OWASP - Informationsbeschaffung zu Mitarbeiterdaten und E-Mail-Adressen - Auswertung durch Identifizierung, Klassifizierung und Priorisierung automatisiert und manuell - Berichterstellung mit Zusammenfassung und technischen Report, Bewertung nach Kritikalität und Eintrittsrisiken - Retests nach Beseitigung der Schwachstellen durch Auftraggeber

CLAUSOHM. Software++ Automation

Clausohm-Software GmbH
Neubrandenburger Str. 46
D - 17039 Neverin
Tel : +49 39 608 26 90 00

www.clausohm.de

Kommunaler IT-Aufgabenträger / Stadt Neubrandenburg /Landkreis Vorpommern-Greifswald / Landkreis Mecklenburgische Seenplatte	- Sicherheitsüberprüfung IT-Infrastruktur
Ansprechpartner	- Frank Papendorf (Informationssicherheitsbeauftragter)
Umfang	- Schwachstellenanalysen von über 100 IP-Adressen und (Sub-) Domains über den kommunalen IT-Aufgabenträger
Umsetzung	- Durchführung vorbereitender Maßnahmen wie Kickoffs, Klärung Ansprechpartner und Eskalationswege, Bestimmung Ziele und Ablauf - Informationsbeschaffung durch Portscans, Schwachstellenscans und Webanwendungsscans mit den Standards nach BSI und OWASP - Auswertung durch Identifizierung, Klassifizierung und Priorisierung automatisiert und manuell - Berichterstellung mit Zusammenfassung und technischen Report, Bewertung nach Kritikalität und Eintrittsrisiken - Retests nach Beseitigung der Schwachstellen durch Auftraggeber und fachliche Unterstützung bei Behebung

CLAUSOHM. Software++ Automation

Clausohm-Software GmbH
Neubrandenburger Str. 46
D - 17039 Neverin
Tel : +49 39 608 26 90 00

www.clausohm.de

Landkreis Eichsfeld	- Sicherheitsüberprüfung IT-Infrastruktur (Intern und Extern) - Durchführung von Phishing Mailkampagnen
Ansprechpartner	- Matthias Bartel (Sachgebietsleiter)
Umfang	- Schwachstellenanalysen von über 300 IP-Adressen und (Sub-) Domains - Versand Phishing E-Mails an die Mitarbeiter mit Auswertung und Ergebnispräsentation
Umsetzung	- Durchführung vorbereitender Maßnahmen wie Kickoffs, Klärung Ansprechpartner und Eskalationswege, Bestimmung Ziele und Ablauf - Informationsbeschaffung durch Portscans, Schwachstellenscans und Webanwendungsscans mit den Standards nach BSI und OWASP - Auswertung durch Identifizierung, Klassifizierung und Priorisierung automatisiert und manuell - Berichterstellung mit Zusammenfassung und technischen Report, Bewertung nach Kritikalität und Eintrittsrisiken - Retests nach Beseitigung der Schwachstellen durch Auftraggeber und fachliche Unterstützung bei Behebung - Durchführung interner Schwachstellenscans der IT-Infrastruktur mit Zugriffsmöglichkeiten

CLAUSOHM. Software++ Automation

Clausohm-Software GmbH
Neubrandenburger Str. 46
D - 17039 Neverin
Tel : +49 39 608 26 90 00

www.clausohm.de

Hochschule Neubrandenburg	- Sicherheitsüberprüfung IT-Infrastruktur & - Sicherheitsüberprüfung vor Ort - Durchführung Phishing Mailkampagnen
Ansprechpartner	- Beate Block (ZIMT | Zentrum für Informations- und Medientechnologie)
Umfang	- Schwachstellenanalysen von circa 20 (Sub-) Domains und IP-Adressen - Schwachstellenscans von über 100 (Sub-) Domains und IP-Adressen - Einrichtung Monitoringsystem für über 2000 (Sub-) Domains und IP-Adressen - Versand regelmäßiger Phishing E-Mails an die Mitarbeiter mit Auswertung und Präsentation - vor Ort Begehungen zur prüfung auf IT-Schwachstellen und Mitarbeiterverhalten
Umsetzung	- Durchführung vorbereitender Maßnahmen wie Kickoffs, Klärung Ansprechpartner und Eskalationswege, Bestimmung Ziele und Ablauf - Informationsbeschaffung durch Portscans, Schwachstellenscans und Webanwendungsscans mit den Standards nach BSI und OWASP - Informationsbeschaffung zu Mitarbeiterdaten und E-Mail-Adressen - Auswertung durch Identifizierung, Klassifizierung und Priorisierung automatisiert und manuell - Berichterstellung mit Zusammenfassung und technischen Report, Bewertung nach Kritikalität und Eintrittsrisiken - Retests nach Beseitigung der Schwachstellen durch Auftraggeber

CLAUSOHM. Software++ Automation

Clausohm-Software GmbH
Neubrandenburger Str. 46
D - 17039 Neverin
Tel : +49 39 608 26 90 00

www.clausohm.de

Stadtwerke Neubrandenburg	- Sicherheitsüberprüfung IT-Infrastruktur - Sicherheitsüberprüfung vor Ort - Durchführung Phishing Mailkampagnen
Ansprechpartner	- Michael Markefsky (Informationssicherheitsbeauftragter)
Umfang	- Schwachstellenanalysen von circa 20 (Sub-) Domains und IP-Adressen - Versand regelmäßiger Phishing E-Mails an die Mitarbeiter - vor Ort Begehungen zur Prüfung auf IT-Schwachstellen und Mitarbeiterverhalten
Umsetzung	- Durchführung vorbereitender Maßnahmen wie Kickoffs, Klärung Ansprechpartner und Eskalationswege, Bestimmung Ziele und Ablauf - Informationsbeschaffung durch Portscans, Schwachstellenscans und Webanwendungsscans mit den Standards nach BSI und OWASP - Informationsbeschaffung zu Mitarbeiterdaten und E-Mail-Adressen - Auswertung durch Identifizierung, Klassifizierung und Priorisierung automatisiert und manuell - Berichterstellung mit Zusammenfassung und technischen Report, Bewertung nach Kritikalität und Eintrittsrisiken - Retests nach Beseitigung der Schwachstellen durch Auftraggeber und fachliche Unterstützung bei Behebung

Clausohm-Software GmbH
Neubrandenburger Str. 46
D - 17039 Neverin
Tel : +49 39 608 26 90 00

www.clausohm.de

2. Informationsbeschaffung

Die Informationsbeschaffung umfasst die Gewinnung von öffentlich ermittelbaren Informationen und beinhaltet folgende Bereiche:

- Sammlung von Unternehmensdaten
    - IP-Adressen
    - (Sub-) Domains
    - Portfreischaltungen
- Sammlung von MitarbeiterInneninformationen
    - E-Mail Adressen
    - Zugehörige Abteilung, Telefonnummer, usw.
    - Prüfung auf Data Breaches

Im Anschluss wird ein zusammenfassender Bericht erstellt.

Clausohm-Software GmbH
Neubrandenburger Str. 46
D - 17039 Neverin
Tel : +49 39 608 26 90 00

www.clausohm.de

3. Externe Sicherheitsüberprüfung / Penetrationstest

Die Durchführung der Penetrationstests richtet sich allgemein nach den 5 Phasen anhand des vom BSI veröffentlichten Durchführungskonzept für Penetrationstests.

- Vorbereitung
- Informationsbeschaffung und Informationsauswertung
- Bewertung der Information / Risikoanalyse
- Aktive Eindringversuche
- Abschlussanalyse

In Phase 1, Vorbereitung findet die detaillierte Abstimmung mit dem Auftraggeber zu den Zielen, Testtiefen, Testbreiten und mehr statt. Dazu gehören auch Testzeiträume zwecks Überprüfung von Produktivsystemen und die Klärung von Reaktionswegen und Ansprechpartnern bei Problemen und Ausfällen von Systemen durch einen Penetrationstest.

In Phase 2, Informationsbeschaffung und Informationsauswertung wird mit der Sammlung von Informationen (IP-Adressen, Subdomains,…) begonnen. Dies umfasst von Außen (Abschnitt 1) z.B. die Portscans

- Durchführung von TCP-Scans (häufigste Ports und Gesamtabdeckung von 65.536 Ports)
- Durchführung von UDP-Scans (häufigste Ports und Gesamtabdeckung von 65.536 Ports)

zur Klärung potentieller Angriffsvektoren und Überprüfungsbereiche. Für die interne Schwachstellenanalyse (Abschnitt 2) werden Scans der IT-Infrastruktur mit Analyse der Netzwerke, Geräte sowie weiterer Dienste durchgeführt.

In Phase 3, Bewertung der Information / Risikoanalyse werden die gesammelten Informationen bewertet und analysiert. Hierbei werden Zielsetzung und Rahmenbedingungen mit den Prüfschritten abgeglichen und Angriffsziele definiert.

Clausohm-Software GmbH
Neubrandenburger Str. 46
D - 17039 Neverin
Tel : +49 39 608 26 90 00

www.clausohm.de

In Phase 4, Aktive Eindringversuche werden die Systeme aktiv angegriffen.

Aufbauend auf automatisierten Prüfungen werden manuelle Schwachstellenanalysen vorgenommen.

Um einen Angreifer zu imitieren, werden auch eigene Informationen zum jeweiligen Dienst mit Imitierung als Nutzer oder Besucher geprüft. Das Vorgehen dient vor allem dazu, dass die Schwachstellenüberprüfungen alle möglichen Angriffspunkte erkennen und false-positive Meldungen der automatisierten Scans entfernen.

Der Ablauf ist:

- Identifizierung von externen Schwachstellen in der IT-Infrastruktur
    - Prüfung von Schwachstellen aufgrund fehlender Sicherheitsupdates
    - Prüfung von Schwachstellen aufgrund von Fehlkonfigurationen
    - Prüfung auf unsichere Verschlüsselungseinstellungen
    - Prüfung auf veraltete Versionsstände von Software und Diensten
    - Prüfung des Schutzes von Zugangsdaten
- Identifizierung von Schwachstellen anhand Kritikalität und Eintrittsrisiko

Die Sicherheitsanalyse beinhaltet damit die umfassende Aufdeckung von Sicherheitsschwächen und die Gefährdungsüberprüfung. Dazu können gehören:

- Überprüfung webbasierter Angriffsmöglichkeiten wie XSS, Code-Injektionen und weiterer
- Überprüfung von Sicherheitsfehlkonfigurationen, wie z.B. falsch konfigurierte HTTP-Header
- Überprüfung Nutzermanagement (Login, Registrierung, Suchfelder,…)
- Überprüfung Software-Versionen
- Prüfung von Sicherheitslücken nach Industriestandard CVE
- Webtesting nach OWASP-Standard

Schwachstellenanalysen im Bereich von Webanwendungen werden zusätzlich nach der Vorgehensweise des Open Web Application Project (OWASP) zum Web Security Testing Guide unterstützt. Hierbei werden wieder Arbeitspakete definiert. Diese können mit dem BSI Leitfaden abgeglichen und die Tests entsprechend erweitert werden.

In Phase 5, Abschlussanalyse wird ein Ergebnisbericht erstellt. Dieser umfasst:

Darstellung Zielsetzung mit Testspezifikationen

- Zusammenfassung für die Geschäftsführung
- Darstellung von gefundenen Schwachstellen mit technischer Beschreibung und darauffolgender Ausführung von Empfehlungen

4. Externes IT-Monitoring

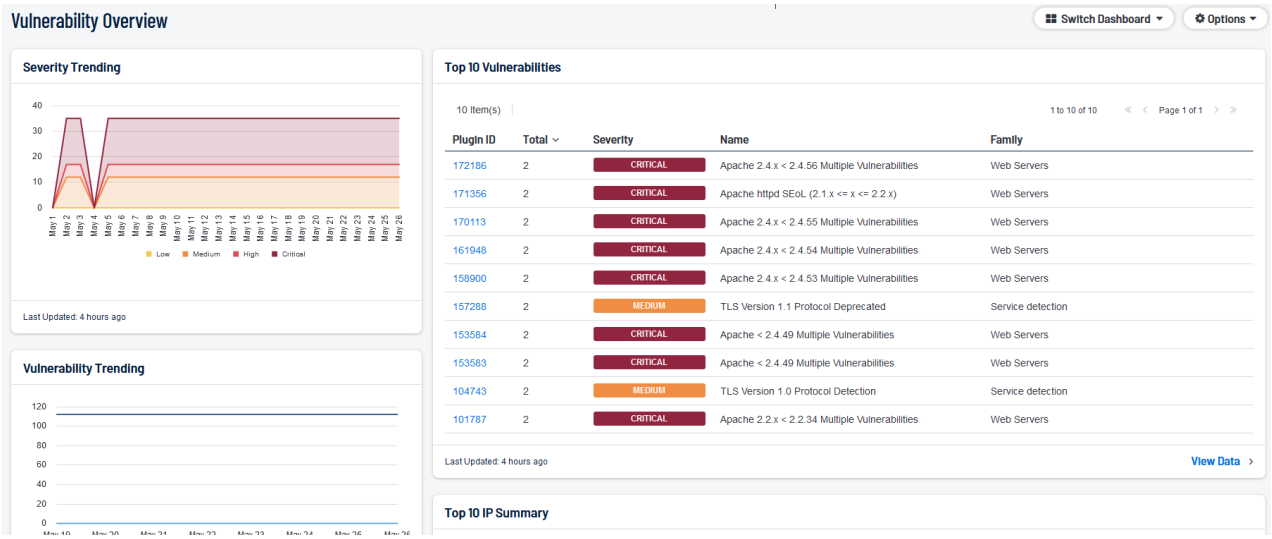
Unser Monitoring as a Service ist unsere Lösung für eine zuverlässige Absicherung Ihrer IT-Systeme gegen Ausfälle und Überlastungen. Wir bieten umfassende Überwachungsdienste für die wichtigsten IT-Ressourcen, darunter Software und Netzwerke. Unser Ziel ist es, potenzielle Probleme frühzeitig zu erkennen und proaktiv zu beheben, bevor sie sich zu ernsthaften Störungen entwickeln können.

Das externe IT-Monitoring bezieht sich auf die Überwachung und Bewertung von IT-Systemen, Netzwerken und Anwendungen von außerhalb der internen Infrastruktur einer Organisation. Es ermöglicht, potenzielle Schwachstellen und Bedrohungen zu identifizieren, die von außen auf die Systeme einwirken könnten. Durch den Einsatz kann auf potenzielle Sicherheitsbedrohungen frühzeitig reagiert werden.

Die Schlüsselkomponenten sind:

- Früherkennung von Problemen
- Optimierung der Leistung
- Verbesserung der Sicherheit
- Integration mit internem Monitoring

Übersicht Gefährdungen



In der Abbildung sind verschiedene Anzeigen zur Übersicht von Gefährdungen und der Bearbeitung sichtbar.

CLAUSOHM. Software++ Automation

Clausohm-Software GmbH
Neubrandenburger Str. 46
D - 17039 Neverin
Tel : +49 39 608 26 90 00

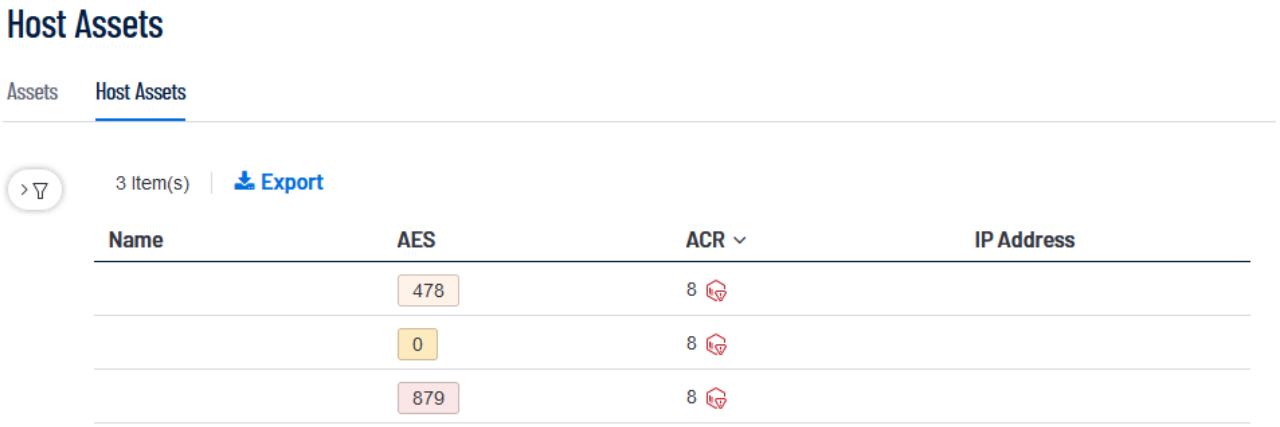
www.clausohm.de

Übersicht Handlungsempfehlungen

Solution	Risk Reduction	Hosts Affected
Upgrade to Apache version 2.4.56 or later.	86.60%	1
Fix TLS Version 1.1 Protocol Deprecated	0.74%	2
Fix TLS Version 1.0 Protocol Detection	0.74%	2
Fix SSL RC4 Cipher Suites Supported (Bar Mitzvah)	0.37%	1

Darstellung der Anzeige von Handlungsempfehlungen zur Behebung der Gefährdungen.

Übersicht IT-Infrastruktur



Auflistung der Anzeige von zu scannenden Werten in der IT-Infrastruktur

Clausohm-Software GmbH
Neubrandenburger Str. 46
D - 17039 Neverin
Tel : +49 39 608 26 90 00

www.clausohm.de

5. Interne Sicherheitsüberprüfung / Internes IT-Monitoring

Im Rahmen der internen Sicherheitsüberprüfung wird ein Monitoring System im internen Netzwerk der Einrichtung eingebunden um für eine bestimmte Zeitdauer das lokale Netz sowie angebundene IT-Systeme zu scannen. Es werden damit Schwachstellen gescannt und die Organisation sowie Netzwerkstruktur dokumentiert.

Entsprechend der Ergebnisse werden Handlungsempfehlungen dokumentiert und Beratungen angeboten. Tritt ein Sicherheitsvorfall auf, unterstützt der Auftragnehmer die Einrichtung bei Aufarbeitung und Einschätzung der Risikolage.

Über eine VPN-Verbindung oder vor Ort über einen angebundenen Thin-Client wird das Monitoring System eingerichtet. Je nach Anforderungen und Größe wird ein entsprechender Zeitraum vereinbart. Die Überprüfung findet mit den folgenden Schritten statt:

- Auftragsklärung
  - Zeitraum
  - Zielsetzung
  - Vorstellung Einsatz Tools
- Informationsbeschaffung
  - Ermittlung der Netzwerkstruktur und der angebundenen IT-Systeme durch Befragung und direkte Scan-Tätigkeiten (Host Discovery, Network Scans)
  - Ermittlung vorhandener Dokumentationen
- Schwachstellenscans
  - Klärung und Durchführung Scans der Netzwerkstruktur
  - Scans der angebundenen IT-Systeme
- Ergebnisanalyse
  - Erstellung Gesamtübersicht mit Klassifizierung entsprechend Sicherheitsniveaus
  - Darstellung Scanergebnisse und Darstellung Prüfung Dokumente
  - Bewertung siehe Schritt 2-2 aus Kapitel 4
- Bericht
  - Freischaltung Dashboard
    - Erstellung Ergebnisanalyse mit Darstellung in Dashboards
      - Freischaltung Zugang als Nutzer
    - Darstellung IT-Landschaft
    - Schwachstellenmanagement
      - Klassifizierung entsprechend Risikoeinschätzung
      - Bereitstellung Reports

Clausohm-Software GmbH
Neubrandenburger Str. 46
D - 17039 Neverin
Tel : +49 39 608 26 90 00

www.clausohm.de

6. Interner Penetrationstest

Die Zielsetzung ist ein direkter Angriffsversuch auf die IT nach Erhalt von Logindaten. Dabei werden nach erfolgreichen Logins Maßnahmen ergriffen, um auf weitere IT-Systeme sowie Daten zuzugreifen.

"Wie weit kann ich mich bewegen? / Was kann ich herausfinden?"

Nach Erhalt möglicher Logindaten von Mitarbeitern werden folgende Arbeitsschritte durchgeführt:

- Login VPN / Zugriff Netzwerk
  - Durchführung weiterer IPScans
  - Einsatz von Reconnaissance und Discovery Tools
- Erweiterung Dateneinsicht
  - Versuch Datenabgriff
  - Versuch Rechteänderung
- Durchführung weiterer Loginversuche

Weiterführende Maßnahmen oder Datenänderungen werden erst nach vorheriger Absprache vorgenommen.

Clausohm-Software GmbH
Neubrandenburger Str. 46
D - 17039 Neverin
Tel : +49 39 608 26 90 00

www.clausohm.de

7. Social Engineering

Das Social Engineering beinhaltet eine Awarenesskampagne mit dem Versenden einer Phishing-Mails an Ihre Mitarbeiter und einer darauffolgenden Auswertung. Die Phishing-Mail beinhaltet einen Querverweis auf eine Website zur Eingabe von Zugangsdaten / personenbezogenen Daten oder zur Möglichkeit eines Dateiuploads.

- Erstellung einer Mail-Kampagne mit Versand an MitarbeiterInnen
  - Erstellung Fake E-Mail Absendeadresse
  - Erstellung Fake-Landingpage
  - Erstellung Fake E-Mail Anschreiben
- Auswertung und Ergebnispräsentation mit Darstellung
  - Zielsetzung
  - Ergebnisse
  - Handlungsempfehlungen

8. Schulung der Mitarbeiter

Mit gezielten Trainings und Workshops sensibilisieren wir Ihre MitarbeiterInnen für mehr Cybersicherheit in Ihrem Unternehmen. Dadurch erhöhen wir nicht nur das Wissen um mögliche Risikofaktoren, sondern stärken gleichzeitig das eigene Sicherheitsgefühl Ihrer Mitarbeiter.

Die Themen der Veranstaltungen reichen dabei von Vorträgen bis hin zu Workshops und praktischen Übungen. Die Inhalte werden entsprechend dem Teilnehmerkreis angepasst und können vor Mitarbeitern sowie Führungskräften und Geschäftsführung durchgeführt werden.

Eine mögliche Schulung kann wie folgt aufgebaut werden:

- Thematik Cyber Security
  - Beispiele bekannte Cyber Angriffe via Social Engineering
  - Vorstellung Cyber Gefahren und deren Gründe
- Thematik Social Engineering
  - Was sind Gründe für das Social Engineering
  - Weitere Beispiele von Phishing Mails (interaktiver Teil mit Teilnahmemöglichkeit)
  - Varianten des Social Engineering
- Live Hacking
  - Vorstellung Durchführung einer Mailkampagne
  - Vorstellung Gefahren eines schlechten Passwortes
- Gegenmaßnahmen
  - Vorstellung von Handlungsempfehlungen im privaten wie beruflichen Umfeld

Clausohm-Software GmbH
Neubrandenburger Str. 46
D - 17039 Neverin
Tel : +49 39 608 26 90 00

www.clausohm.de

9. Vortragsreihe

Es stehen vier spezifische Vorträge für die Zielgruppen

- Schüler und Lehrkräfte,
- Unternehmen und Mitarbeiter
- und Kommunen und Ämter bereit.

Vortrag #1 umfasst das Thema „Schutz vor Cyber-Kriminalität“ mit den Inhalten:

- Schutz vor Phishing E-Mails
- Schutz des Online Bankings / Online Shopping
- Soziale Netzwerke: Sicherer Umgang mit sozialen Netzwerken, Sicherheitseinstellung bei Facebook, Whatsapp und Co
- Erste Hilfe im Notfall

Vortrag #2 umfasst das Thema „Kinderschutz im Internet“ mit den Inhalten:

- Technischer Schutz für Kinder im Internet: Nutzungszeiten, Internetinhalte, Sperrung von Diensten, Netzwerkstrukturen usw.
- Schutzmaßnahmen für Kinder im Internet: Umgang mit Spam, Phishing, Schadprogramme, Downloads, persönliche Informationen usw.

Vortrag #3 umfasst das Thema „IOT + Smarthome“ mit den Inhalten:

- Das Internet der Dinge -Gefährdung und Beispiele
- Sicherheitsstrategien für unser SMART-HOME
- Verhalten im öffentlichen WLAN
- Smartphone und Tablet sicher nutzen

Vortrag #4 umfasst das Thema „Cyber Security for Teenies“ mit den Inhalten:

- Sicher online am Start
- Password Swordfisch
- Social Media & Chats
- Cybergrooming

Die Dauer beträgt jeweils 30 bis 45 Minuten und kann Online oder vor Ort durchgeführt werden.

Clausohm-Software GmbH
Neubrandenburger Str. 46
D - 17039 Neverin
Tel : +49 39 608 26 90 00

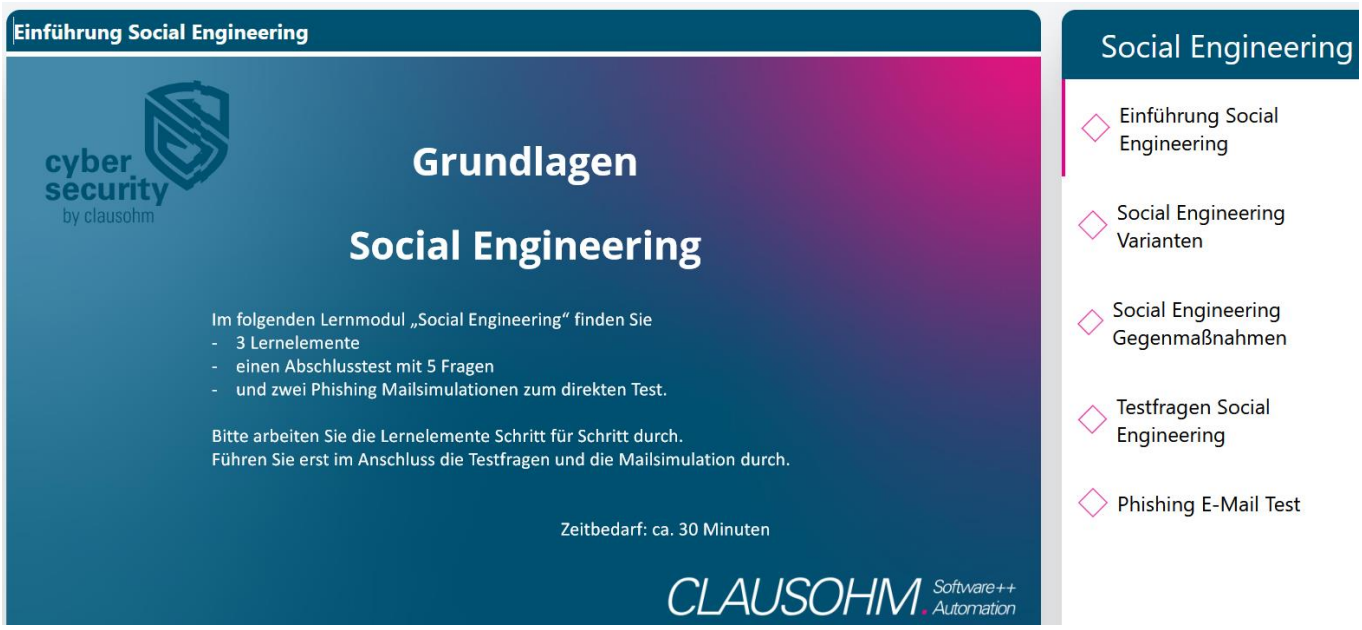
www.clausohm.de

10. Lernplattform AWAP

Schulungen der Mitarbeiter können durch unsere Lernplattform AWAP geschehen. In Lernmodulen werden

- Lernelemente,
- Multiple-Choice Tests
- sowie interaktive Phishing Mailsimulationen von Mitarbeitern bearbeitet.

Die Dauer zur Bearbeitung der jeweiligen Lernmodule betragen höchstens 30 Minuten und nach erfolgreichem Abschluss erhalten die MitarbeiterInnen ein Zertifikat.



In der Abbildung wurde nun das Lernmodul Social Engineering ausgewählt. Auf der rechten Seite werden die Lernelemente angezeigt. In dem Beispiel besteht die aus

- 3 Lernelementen (Lernmodul, Varianten, Gegenmaßnahmen),
- einer Fragerunde (Multiple-Choice-Test aus den Inhalten der Lernelemente)
- und eine Phishing E-Mail Simulationen zum Test

Abbildung 1: Auswahl Lernmodul

Clausohm-Software GmbH
Neubrandenburger Str. 46
D - 17039 Neverin
Tel : +49 39 608 26 90 00

www.clausohm.de

11. Live Hacking

Als Alternative zu den Schulungen bieten unsere Live Hacking Events praxisnahe Einblicke zu Angriffsmöglichkeiten von Hackern. Die Events können spezifisch angepasst werden und können aus folgenden Szenarien bestehen:

- Einleitung
  - Vorstellung aktueller Bedrohungen im Cyberraum
  - Vorstellung dokumentierter Cyber Angriffe mit regionalen Bezug
- Hauptteil
  - Durchführung einer Phishing E-Mailkampagne am Beispiel mit Unterstützung durch Künstliche Intelligenz (KI)
  - Vorstellung der Einsatzmöglichkeiten schadhafter USB-Sticks (Rubber Ducky=
  - Durchführung einer Passwortermittlung am Beispiel über die Informationsbeschaffung durch Social Media
  - Durchführung von Voice Cloning am direkten Beispiel
  - Durchführung von technischen Angriffe auf eine Webanwendung
- Schlussteil
  - Vorstellung von Handlungsempfehlungen zum Schutz vor Cyber Angriffen

Clausohm-Software GmbH
Neubrandenburger Str. 46
D - 17039 Neverin
Tel : +49 39 608 26 90 00

www.clausohm.de

12. Beratung und Risikoanalyse

Wir unterstützen Sie aktiv in der Erarbeitung von IT-Sicherheitsrichtlinien und Handlungsempfehlungen bis hin zur Begleitung von Zertifizierungsmaßnahmen nach ISO:27001 oder IT-Grundschutz. Wir sind zur Durchführung von Cyber-Sicherheits-Checks, im Rahmen des vom BSI und ISACA Germany Chapter e. V. in Kooperation veröffentlichten Leitfadens zertifiziert und begleiten Sie auf dem Weg zu notwendigen Auditierungen.

Die NIS-2-Richtlinie gilt ab Oktober 2024 für viele Unternehmen und Organisationen in 18 kritischen Sektoren und wird in Zukunft zu verpflichtenden Sicherheitsmaßnahmen und Meldepflichten – auch für viele, die bisher nicht betroffen waren – führen. Die Anforderungen der NIS-2-Richtlinie umfassen Maßnahmen zur Senkung von Risiken für die Sicherheit der Informationssysteme. Ein früher Beginn der Bearbeitung von NIS2 Anforderungen ermöglicht zudem, dass die Umsetzung zielorientiert und praxisnah umgesetzt werden können

Wir bieten umfassende Beratung im Bereich Business Continuity Management, um die Fortführung kritischer Geschäftsprozesse während Krisen zu gewährleisten. Unser Ansatz schließt Risikoanalysen, Impact-Bewertungen sowie regelmäßige Tests und Schulungen ein, um die Resilienz von Unternehmen zu stärken und Compliance sicherzustellen.

Clausohm-Software GmbH
Neubrandenburger Str. 46
D - 17039 Neverin
Tel : +49 39 608 26 90 00

www.clausohm.de

13. Weitere Leistungen

13.1 Überprüfung Software

Hierbei werden die sicherheitsrelevanten Funktionen auf Schwachstellen im Quellcode und im direkten Test analysiert. Mit Zugriff auf ein bereitgestelltes Software-/ Kundensystem werden verschiedene Angriffsvektoren kontrolliert. Dies kann die Möglichkeiten zu Rechteausweitungen, Datenbank-Injections oder das Umgehen von Schutzmechanismen beinhalten. Mit Bereitstellung des Softwarecodes kann hier eine entsprechende Codeanalyse durchgeführt werden.

Das Arbeitspaketsetzt sich aus den folgenden Arbeitsschritten zusammen:

- Schwachstellenanalyse Softwareprodukt
- Schwachstellenanalyse Softwarecode
    - Statische Codeanalyse
    - Verifikation und manuelle Prüfung sicherheitsrelevanter Funktionen
    - Dynamische Codeanalyse

13.2 Schulungen zum Einsatz Künstlicher Intelligenz (KI) im Unternehmensumfeld

Unser Hauptanliegen ist es, die Geschäftsführung umfassend über den Mehrwert aufzuklären, den der Einsatz von KI-Technologien mit sich bringt. Unser Angebot umfasst dabei insbesondere die Darlegung von Do's and Dont's im Umgang mit KI, die Vorstellung vielfältiger Anwendungsmöglichkeiten in den unterschiedlichen Unternehmensbereichen, die Beachtung von Datenschutz- und IT-Sicherheitsaspekten sowie eine Kostenübersicht.

Darüber hinaus streben wir darauf an, Mitarbeiterinnen und Mitarbeiter so zu schulen, dass sie KI-Technologien sicher und wirkungsvoll in ihren Arbeitsalltag integrieren. Unsere Schulungen verstärken das Verständnis und die Handhabung von KI-Werkzeugen und demonstrieren, wie diese Technologien Produktivität sowie Arbeitsqualität verbessern können. Gleichzeitig tragen diese Bildungsmaßnahmen zur Gewährleistung der