oneconsult
together against cyberattacks

Penetration Tests als Selbstverständlichkeit - auch in öffentlichen Verwaltungen

Roman Vogt, Oneconsult AG | Webinar DVS, 29. Mai 2024

Roman Vogt

Head of Red Teaming & Penetration Testing

CISSP, CEH

T: +41 43 377 22 12

M: +41 79 675 65 55

E: roman.vogt@oneconsult.com

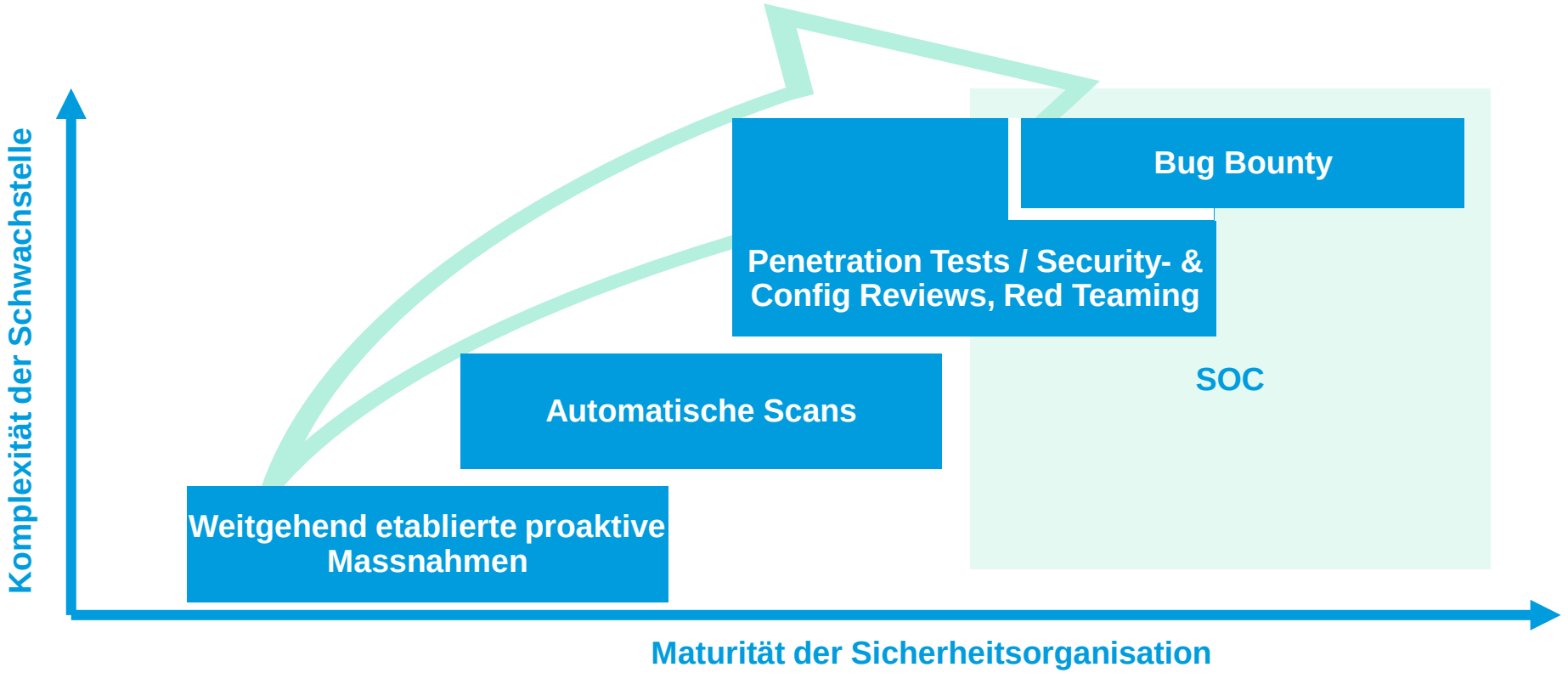
Agenda / Inhaltsverzeichnis
Penetration Tests als Selbstverständlichkeit

Proaktive Security Massnahmen

Einordnung und Übersicht von Penetration Tests

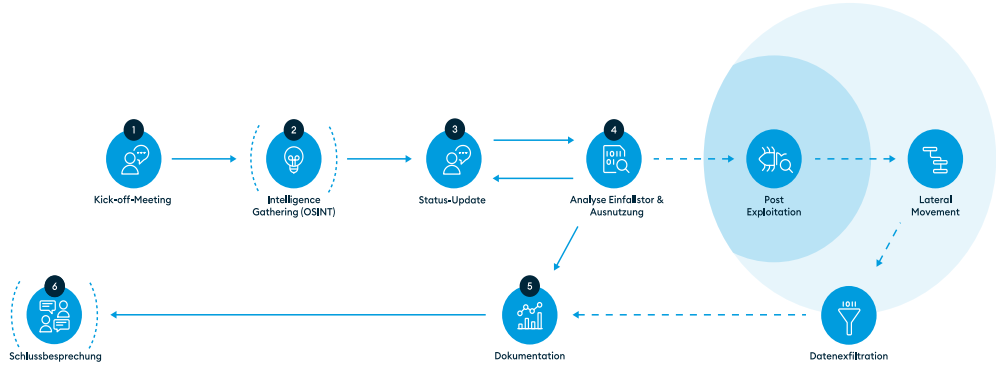
Proaktive Massnahmen

Zur Erhöhung der Cyber-Resilienz sollen verschiedene proaktive Massnahmen ergänzend etabliert und die Maturität laufend verbessert werden:



Penetration Tests / Security Reviews / Config Reviews

Bei **Penetration Tests**, auch Pentests genannt, werden geeignete Mittel und Methoden eingesetzt, **um vorhandene Schwachstellen aufzudecken**. Ob unbefugtes Eindringen in Systeme, Möglichkeiten zur Datenmanipulation oder unsichere Anwendungen – ein Pentest deckt **systematisch und strukturiert** Sicherheitsmissstände auf. Anschliessend wird ein **Bericht** erstellt, der zeigt, wo und welche **Risiken** bestehen und **wie diese behoben werden** können.



Bei einem **Security Assessment** wird **zusätzlich** zum Penetration Test auch die **Konfiguration** des Systems sowie der **operative Umgang** mit dem System bewertet.

Beim **Configuration Review** wird die **Konfiguration** des Systems auf **sicherheitsrelevante Einstellungen** geprüft. Dabei werden zum Beispiel **Abweichungen** von Implementierungs- oder **Sicherheitskonzepten** identifiziert.

Penetration Tests / Security Reviews / Config Reviews - Überblick

Penetration Testing

Application Testing

- Web Application Penetration Test
- API Penetration Test (REST, SOAP etc.)
- Application Penetration Test (Client- / Server Application)
- Mobile App Penetration Test
- Code Review (Application Security)

Network- / Security Infrastructure Testing

- Security- / Vulnerability Scan (Network / Infrastructure)
- System Penetration Test
- Firewall Security Assessment
- Wireless LAN Security Assessment (WLAN)
- E-mail Security Assessment
- VoIP / UC Security Assessment
- Remote Access Security Assessment

Client- / Server Infrastructure Testing

- Client Security Assessment (Windows, Unix, VDI)
- Server Security Assessment (Windows, Linux / Unix)
- Active Directory Security Assessment
- Container Security Assessment
- Security Configuration Review
- Mobile Device Security Assessment (incl. MDM)

Cloud Security Testing

- M365 & MS Teams Security Assessment
- Microsoft Entra ID Security Assessment
- Azure Security Assessment
- AWS Security Assessment (Amazon Web Services)
- GCP Security Assessment (Google Cloud Platform)
- Cloud Security Assessment (Non-Hyperscaler)

IoT & OT Security Testing

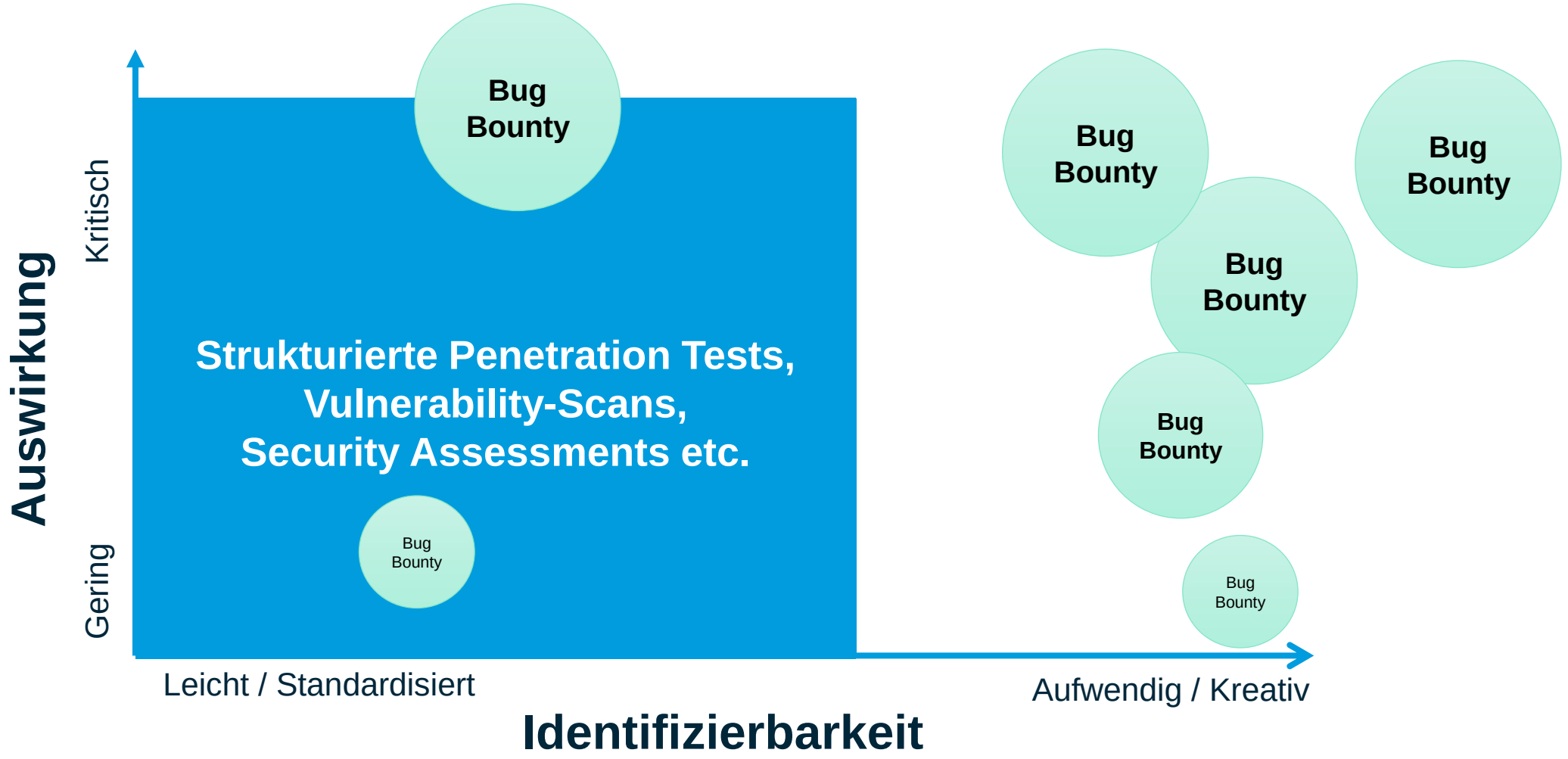
- IoT Penetration Test
- ICS: SCADA / DCS Penetration Test
- IoT Security Assessment
- OT Security Assessment
- Wireless / Embedded Devices / Protocols etc.

Red Teaming

Attack Simulation & Social Engineering

- Red Teaming (Technical Attack Simulation)
- Purple Teaming (Know-how Transfer & Attack Simulation)
- OSINT Assessment
- Social Engineering
- Physical Access Assessment
- Phishing Simulation / Spear Phishing

Systematische und kreative Schwachstellensuche
Penetration Tests & Bug Bounty ergänzen sich



Erfahrungsbericht

Penetration Test / Security Assessments aus Sicht verschiedenen Stakeholdern

Erfahrungsbericht & aktuelle Bedrohungssituation

Erfahrungsbericht

Systemverantwortliche haben eher Angst, dass etwas Aufgedeckt wird, was sie selber hätten sehen müssen

Aufwendige Bereitstellung für Tests

Keine Zeit für Pentest oder Security Assessment – Usability / Funktion wichtiger

ISDS-Konzepte oft nicht aus einer Hand, Interpretationsspielraum, Schutzmassnahmen eher nur teilweise umgesetzt

«Unnötig, wir wissen schon, was wir tun» - «Misstrauens-Votum»

Nur Penetration Test, wenn explizit von CISO / ITSIBE gefordert

Zu viele andere wichtige Dinge, Projekte, Betrieb etc.

Erfahrungsbericht:
Penetration Tests aus Sicht von…

…System- und Anwendungsverantwortlichen

- *«Ist für den CISO / ITSIBE / Auditor»*
- *«Unnötig, wir wissen schon, was wir tun»*
- *«Die vertrauen uns nicht – jetzt werden wir geprüft / getestet»*
- *«Ich habe wichtigeres und dringenderes zu tun»*
- *«Wir haben gute Firewalls und Zonierungen, das genügt»*
- *«Unser System ist so speziell, das kann nicht von Externen getestet werden»*

Erfahrungsbericht:
Penetration Tests aus Sicht von…

…Budgetverantwortlichen

- *«PT hatte ich bisher nie Budgetiert – Budgeterhöhungen chancenlos»*
- *«Das muss «in der Security»
  «im Projekt»
  «im Betrieb» budgetiert werden».*
- *«Kann nicht beurteilen, wie viele Penetration-Tests für welche Anwendungen und Systeme nötig sind – und mit welchem Aufwand zu rechnen ist»*
- *«Welche Security Massnahme wird im Gegenzug gestrichen?»*
- *…*

Erfahrungsbericht:
Penetration Tests aus Sicht von…

…Beschaffungsstelle

- *«Da muss zuerst eine Ausschreibung gemacht werden»*
- *«Das benötigt einen Rahmenvertrag mit diversen Partnern und anschliessenden Mini-Tender»*
- *«Im fernen Ausland sind Penetration Tests viel günstiger»*
- *«Das müssen doch die Lieferanten von Systemen / Anwendungen selber Testen»*

Aktuelle Bedrohungssituation

Erfahrungsbericht & aktuelle Bedrohungssituation

Aktuelle Bedrohungen

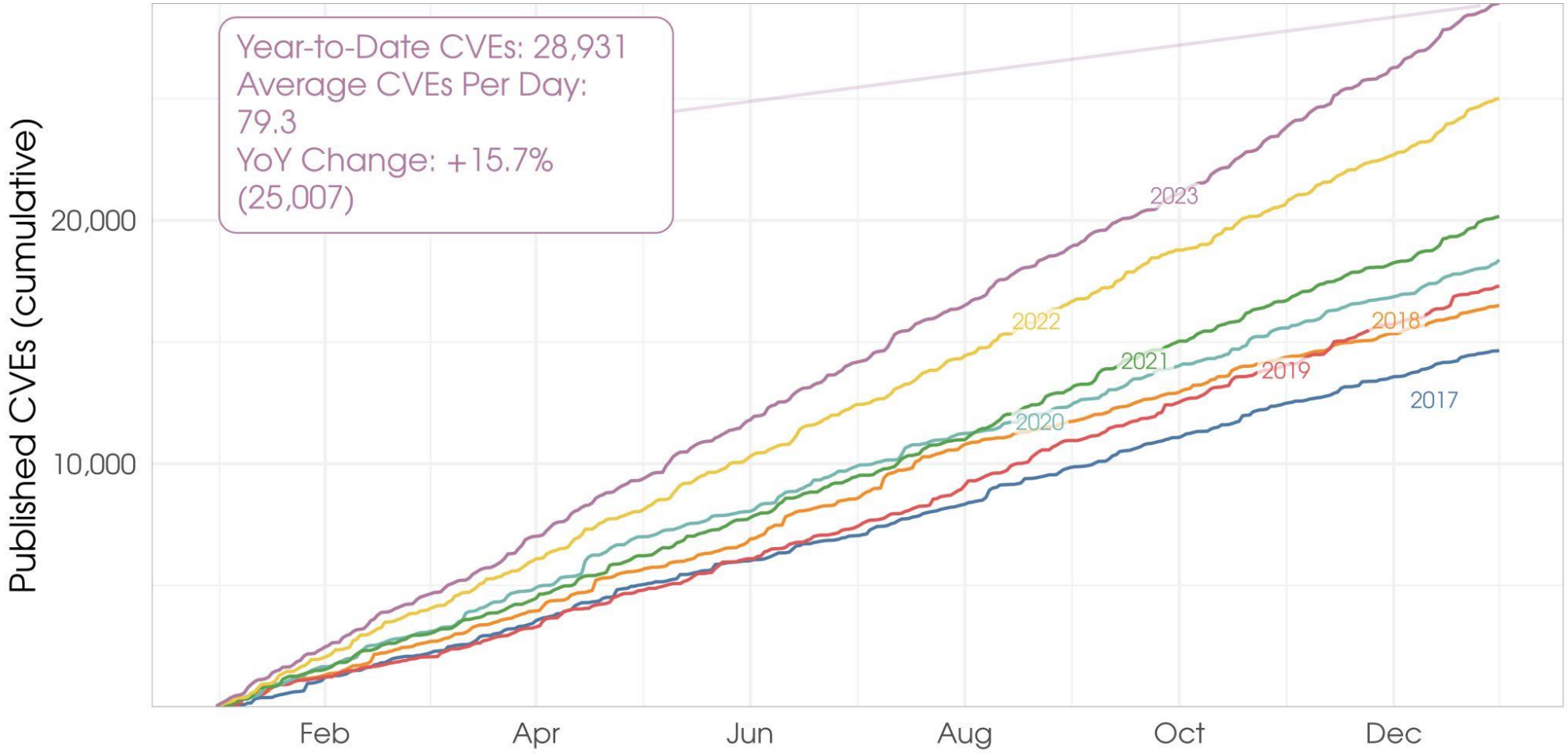
- Phishing (Vishing, Smishing)
- Datenabfluss
- Ransomware
- CEO-Betrug (KI-Unterstützt)
- Risiken durch Supplier Chain / Lieferantenkette
- DDoS
- …

Siehe auch: Die häufigsten Sicherheitslücken, Penetration Testing (youtube.com)

Erfahrungsbericht & aktuelle Bedrohungssituation

Year-to-date CVE publications (MITRE CVE List)

Lines showing the daily cumulative count of published CVEs on MITRE's CVE List, https://cve.mitre.org/cve/



Source: https://first.org/epss/data_stats, 2024-01-01

Auf dem Papier «alles gut»

Auf dem Papier «alles gut» Schuban, ISDS-Konzepte, ISO 27001 etc.

Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept)

Ergibt die Schutzbedarfsanalyse einen erhöhten Schutzbedarf, so definieren die Verwaltungseinheiten, zusätzlich zur Umsetzung der Sicherheitsvorgaben für den Grundschutz und basierend auf einer Risikoanalyse, weitere Sicherheitsmassnahmen, dokumentieren diese und setzen sie um. Das ISDS-Konzept beinhaltet die Beschreibung der Sicherheitsmassnahmen und ihre Umsetzung für das Informatikschutzobjekt sowie der Restrisiken.

ISO 27001

Organisationen, die ISO 27001 zertifiziert sind, überprüfen regelmässig, ob ihr Informationssicherheits-Managementsystem (ISMS) den Anforderungen der ISO/IEC 27001 entspricht. Der Standard beschreibt die Implementierung und Dokumentation eines ISMS, um Sicherheitsrisiken zu minimieren und langfristig die Qualität der IT-Systeme zu optimieren

Auf dem Papier «alles gut»
Schuban, ISDS-Konzepte, ISO 27001 etc.

Herausforderungen

- Zeitbedarf für Umsetzung
- Technische und fachliche Komplexität
- Abhängigkeiten (ZB. Einschränkungen Usability, Umsysteme)
- Unrealistische Massnahmenvorschläge (Time, Budget, Functionality)
- Fehlende Expertise

Dies kann dazu führen, dass beschriebene und dokumentierte Sicherheitsmassnahmen nicht oder unvollständig umgesetzt werden!

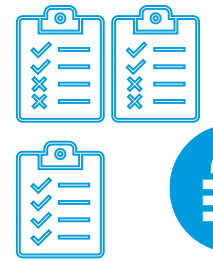
Penetration Tests und Security-Assessments als Entlastung

Beruhigt in die Ferien

Penetration Tests und Security-Assessments als Entlastung

Penetration Tests als Freunde der System- und Anwendungsverantwortlichen

- Mit jedem Test / Testresultate gewinnt man an Know-How für zukünftige Implementationen / Konfigurationen
- Meine Anwendung / Mein System wird mit Umsetzung der Massnahmen sicherer – beruhigende Wirkung
- Ich will es wirklich wissen (eigener Ehrgeiz)
- Vergleichsmöglichkeiten mit anderen durch standardisierte RAV-Werte
- Konkrete Massnahmen-Empfehlungen zur Behebung



Penetration Tests und Security-Assessments als Entlastung

Penetration Tests als Freunde der System- und Anwendungsverantwortlichen

- Gewissheit, es wird das Möglichste unternommen, damit nicht ein krimineller Hacker Schaden über «mein System» verursacht
- Bei mehrjähriger Zusammenarbeit wird jedes Projekt einfacher
- Je nach Anbieter, cooler Austausch und mögliche Sessions zusammen mit Ethical-Hacker / Pentester
- Zusammen etwas gegen Cyberattacken / Cyberkriminalität zu unternehmen (Wir-Gefühl in einer wichtigen und guten Aufgabe)




Empfehlungen für IT-Projekte und IT-Betrieb

Empfehlungen für IT-Projekte und IT-Betrieb

Empfehlungen für Projekte (Projektleiter, Sponsor, Projektmitarbeitende)

- Penetration Tests / Sicherheitstest in Standard Projektvorgehen integrieren
  - Prozesse
  - Dokumentvorlagen
  - Hermes nutzen / Hermes Vorlagen bedarfsgerecht ergänzen
- Fast jedes IT - Projekt braucht Security-Budget

Als fester Bestandteil in Projektbudgetantrag aufnehmen

- In Projektauftrag (PA/PIA/etc.) bereits an Sicherheit denken und in Ziele, Ressourcen-bedarf, Termine, Rahmenbedingungen etc. berücksichtigen / Thematisieren
- Massgebende Mitwirkung von System-verantwortlichen (SE/DEV) auch bei allen sicherheitsrelevanten Dokumenten / Konzepten wie Systemarchitektur, Sicherheitskonzept, Schuban, ISDS-Konzept.

Jeweils das Testen der Cyber-Resilienz im Projektplan vorsehen, zusammen mit Betroffenen planen, die Tests begleiten und Findings für den weiteren Projektverlauf berücksichtigen

Empfehlungen für IT-Projekte und IT-Betrieb

Empfehlungen für **Budgetverantwortliche und Beschaffungsstelle**

- **Einzelbeschaffung** von Penetration Tests / Sicherheitstests pro Projekt, Webapp, Website, System, Anwendung…
  - ⊕ Kurzfristig, spezifische Auswahl, unterschiedliche Testansätze, einfache Beschaffung
  - ⊖ Testbereitschaft / Setup, Terminfindung, Scoping - Genauigkeit, Koordination
- Beschaffung über **Rahmenvertrag**
  - ⊕ Prozesse / Zusammenarbeit, Preis, Überblick / Zusammenhänge, Team
  - ⊖ Beschaffungsprozess, Budgetgenauigkeit, Langfristige Planung, wenig Flexibilität für Spezialanforderungen

- Budgetverantwortliche klären **vor der Budgetphase**, wo proaktive Sicherheitsmassnahmen wie Penetration Tests / Sicherheitstest und Bug Bounty budgetiert werden:

  Zentral bei «Security» **oder dezentral** bei Projekt, Betrieb (Anwendungs- / Systemverantwortlichen)

  ☞ Dezentral, in jedem Projekt, jedem System, jeder Anwendung, insbesondere Webanwendung sollte das Thema individuell betrachtet und budgetiert werden.

Empfehlungen für IT-Projekte und IT-Betrieb

Empfehlungen für IT Betrieb / Anwendungsbetrieb (AV, PO, SE, DEV)

- Testbedarf in System-Dokumentationsvorlage
- Tests definieren und fix einplanen
- Resultate / Findings (wo möglich) intern mit anderen teilen
- Hardening-Guidelines nutzen
  Bsp: https://www.cisecurity.org/cis-benchmarks
- Von Anfang an «sicher» gemacht, erspart sehr viel Zeit in Zukunft.
- Positive persönliche Einstellung
- Implementierungszeiten können sich verkürzen, wenn früh Pentests gemacht werden
- Wir sollten nicht nur den Mitarbeitenden vertrauen, sondern auch den Systemen und Anwendungen
- Happy CISO / IT SIBE = Happy Life
- Firewalls und Zonierungen alleine halten nicht von einer erfolgreichen Cyberattacke ab – Es braucht zwingend weitere, ergänzende Massnahmen

Empfehlungen für IT-Projekte und IT-Betrieb

Weitere Antworten und Empfehlungen

«Penetration Tests sind für den CISO / ITSIBE»

Penetration Test sind wesentlich, um die Erhöhung der Cyber-Resilienz zu ermöglichen. Sie sind weder «für den CISO» noch für den Chef.

«Penetration Tests sind unnötig, wir wissen schon, was wir tun»

Bei fast allen betroffenen Firmen von bekannten grossen Sicherheitsvorfällen arbeiten ganz viele sehr gute Fachkräfte. Das allein hilft nicht immer.

«Penetration Tests sind nicht Budgetiert, Budget- Erhöhungen sind chancenlos»

Dia aktuelle und Bedrohungs-situation, Beschleunigung der Anzahl Attacken und CVE’s, sowie neue regulatorische Vorgaben sprechen für sich.

«Welche Security Massnahme streichen?»

Sicherheitsmassnahmen, welche massiv die Usability einschränken und nur eine sehr geringe Sicherheitsverbesserung darstellen. Im Einzelfall gut prüfen!

«Im fernen Ausland sind Penetration Tests viel günstiger»

Qualität, Expertise, automatisierte und manuelle Tests und Methoden, Flexibilität, Beratung, Verlässlichkeit, Daten / Bearbeitung CH und viele Argumente mehr für lokale Anbieter.

«Lieferanten / Hersteller müssen selber testen, ist nicht unsere Sache»

Das wird gemacht. Jedoch sind Systeme / Anwendungen pro Installation und Umsysteme unterschiedlich und deshalb im Systemkontext (Live) zu prüfen.

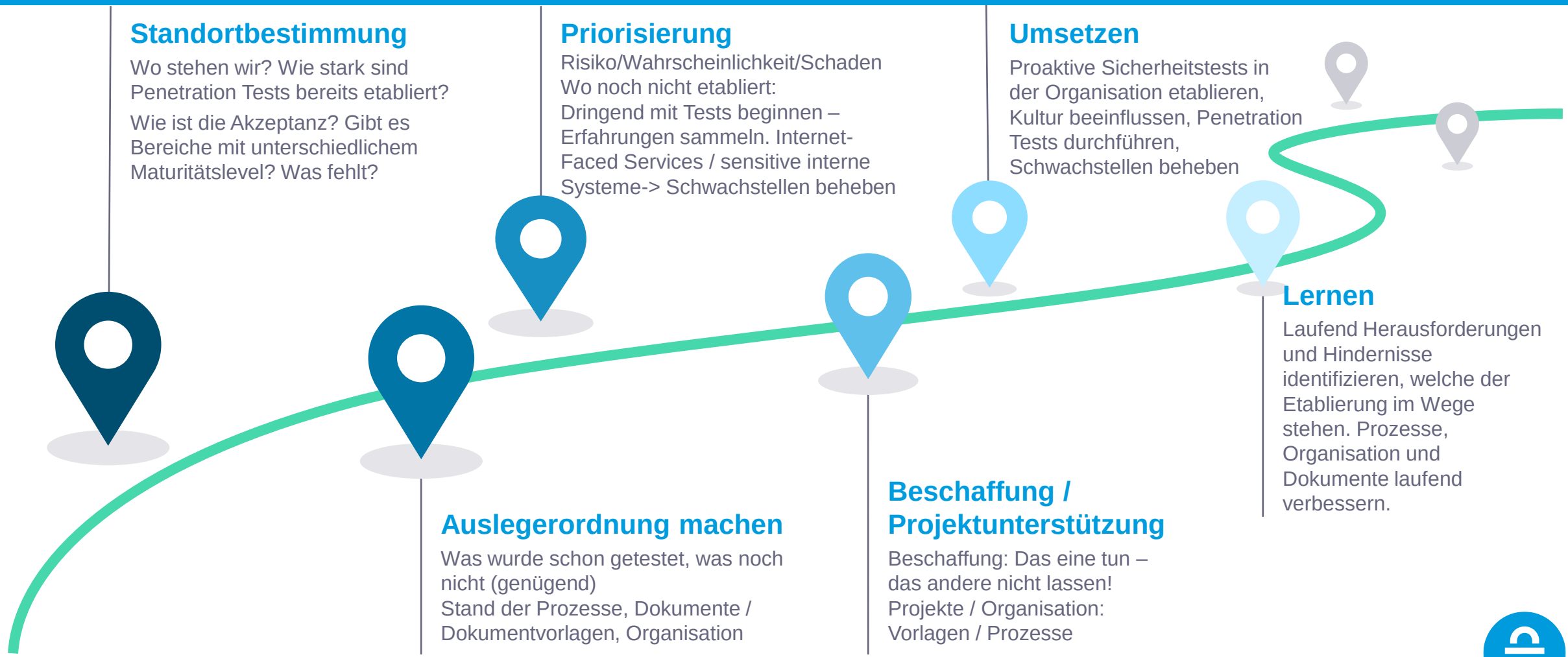
Sicherheitsaudits und Penetration Tests etablieren

Sicherheitsaudits und Penetration Tests etablieren

- Freude am Thema entwickeln, nur sichere Systeme sind gute Systeme
  - prozessuale und formelle Hindernisse reduzieren
- Sicherheitsaudits und Penetration Tests abbilden in Prozessen, Vorlagen, Dokumentationen, Handbücher
- Beschaffungsstelle und Budgetverantwortliche immer und von Anfang an ins Thema Cybersecurity miteinbinden
- «Together against cyberattacks»! Pentests bieten für System-verantwortlichen / Anwendungs-verantwortliche oft die Möglichkeit zum Austausch mit Top-Fachleuten
  - Macht echt Spass und bereichert (von «push» zu «pull»)

Vorgehensempfehlung

Vorgehensempfehlung



Standortbestimmung

Wo stehen wir? Wie stark sind Penetration Tests bereits etabliert?

Wie ist die Akzeptanz? Gibt es Bereiche mit unterschiedlichem Maturitätslevel? Was fehlt?

Auslegerordnung machen

Was wurde schon getestet, was noch nicht (genügend)
Stand der Prozesse, Dokumente / Dokumentvorlagen, Organisation

Priorisierung

Risiko/Wahrscheinlichkeit/Schaden
Wo noch nicht etabliert:
Dringend mit Tests beginnen – Erfahrungen sammeln. Internet-Faced Services / sensitive interne Systeme-> Schwachstellen beheben

Beschaffung / Projektunterstützung

Beschaffung: Das eine tun – das andere nicht lassen!
Projekte / Organisation: Vorlagen / Prozesse

Umsetzen

Proaktive Sicherheitstests in der Organisation etablieren, Kultur beeinflussen, Penetration Tests durchführen, Schwachstellen beheben

Lernen

Laufend Herausforderungen und Hindernisse identifizieren, welche der Etablierung im Wege stehen. Prozesse, Organisation und Dokumente laufend verbessern.

Fragen?

Nutzen Sie für Fragen die Chat-Funktion, falls Voice ausgeschaltet ist

oneconsult
together against cyberattacks

Vielen Dank!

Oneconsult AG | together against cyberattacks

Let's connect

www.oneconsult.com

/oneconsult-ag

/OneconsultAG

/oneconsult

Monatliche Cyber Security News abonnieren:

Oneconsult Newsletter