Pentest Geraffel

Mein Aufbruch in eigentlich bekannte Gefilde…

V1.4 - 26.11.2019

Security Geraffel

Vorwort

… An einem Tag von vor 10 Jahren nach einer Konferenz …

… 3 Männer, 1 Taxi und später Nachmittag …

… eine Diskussion beginnt über die Zukunft von Pentests …

… dabei stehen folgende Thesen im Raum:

- Erweiterung des internen Pentest Teams
- Nutzung externer Pentest Teams

Anmerkung

- Alles was jetzt kommt ist aus meiner eigenen Sichtweise
  - Sichtweise eines Managers und nicht Pentesters
  - Zielsetzung ist nicht nur ein “get it done”, sondern auch ein “get it fixed”
- Die Ausgangslage ist komplett unterschiedlich
  - Anderes Backing, weniger beteiligte Personen
- Es ist kein “Ätsch ich kann es besser”
  - Nö, nur anders und auf meine Art und Weise
- Und es ist nicht DIE Lösung, sondern EINE
  - Wobei sich diese besser skalieren lässt ;)

Ein Neustart

Was ich vorfand

- Am Anfang war das Nichts…
- Kein Template für Reports
- Ein Tracking der Findings, aber **ohne** Eskalation
- Kein JourFix mit CISO und Co. für Reports
- Keine KPI

Aber

wir hatten eine Prozessdokumentation und ein Workflow Diagramm !

Ausgangslage innerhalb der IT

- Unkenntnis bei den TAV (**T**echnische **A**nwendungs**v**erantwortliche)
  - Aber das ist doch verboten !?
  - Ich muss **was** machen ?
- Gefährliches Halbwissen
  - Habe ich bei Cyber CSI mal gesehen
  - Also so wie in Mission Impossible !?
  - Aussage wie Greybox | Whitebox != pentest
- Ignoranz gegenüber Vorgaben aus Security Controls
  - Verstoss gegen GRC (RSA Archer) Controls - Ja und ?
  - Habe besseres zu tun !
  - Lieber ändere ich die Risikoeinstufung, als sowas zu machen !

Herausforderungen

Problem	Lösung
Keine Fremdgeräte	VMWare Workstation
Kundenängste	Präsentationen
Ablehnung / Ignoranz	Geschmacksverstärker
Konservativer Konzern	Regulatorik
EZB Anforderungen	Dokumentieren²
Unabhängige Dritte	7 Pentestfirmen
Interessenkonflikte	Delegieren
BMA	Second Line Aufgabe

Welches IT-Asset ist wichtiger?

- CISO Team Anforderungen vs Realität
  Elfenbeinturm vs Ressourcen (Geld / Zeit / Personen)
- 3 Jahresplanung, basierend auf Prioformel
- Ermittlung Erfüllungsgrad und Restrisiko
- Erstellung Entscheidungsvorlage für Risikoakzeptanz durch Leitung IT
- **Wichtig:**
  100 % Erfüllungsgrad im Zyklus ist nicht machbar !
  Es kommt **immer** was dazwischen !
  Offene Kommunikation ist hier der Schlüssel !
  Begründet wieso ihr ein IT-Asset **nicht** pentesten könnt !

Prio Formel

- Dies ist nur ein Beispiel!

Schutzbedarfsstufe	0 bis 3	Wie wichtig ist es gemäß GRC ?
+ Datenschutzstufe	0 bis 3	Was für Daten sind drin ?
+ Internetfacing	0 oder 1	Scriptkiddi Interface aka Web ?
+ Pentestfindings vormals	0 oder 1	ReTest zu planen ?
+ MAS / HKMA relevant	0 oder 1	Für den Regulator relevant ?
+ Restjahre Zyklus	0 bis 3	Noch Zeit zum aussitzen ?

- Maximal 12 und da Manager gerne von 1 an Zählen…
  Prio = 13 - Ergebnis

Revisionsprüfung

- *Und wo steht das was Sie mir gerade erzählt haben ?*
  Prozess und Workflows dokumentieren
- *Gibt es zur Version 0.9 auch eine Finale und was wurde dort geändert ?*
  Reports finalisieren, Versionshistorie pflegen
- *Was war der Inhalt des Pentests ?*
  Scope und Inhalte sauber ausarbeiten
- *Was wurde gefunden und ist es adressiert oder schon behoben?*
  Trackt eure Ergebnisse und Findings, z.B: Problemtickets
- *Wieso wurde das IT-Asset nicht einem Pentest unterzogen?*
  Habt eine gute Begründung für nicht durchgeführte Pentests

Pentestfabrik als Aufgabe und Ergebnis

- Skalierungseffekte
  - Aktuell mehrere Pentests Parallel machbar
- Jährliche Pentests
  - Zzgl. Projekte und Erfüllung der 3-Jahres Zyklen für andere
- Sinn und Sinnigkeit dahinter
  - Tracking Tickets noch offen, lohnt sich ein erneuter Pentest ?
- Karnickel Pentests (Ticket Bomben) sind keine Lösung
  - Target Bashing - “Ist kaputt, aber lass mal machen”
- Agile vs Pentest (DevSecOP)
  - Runs alle 6 Wochen

Providerlösungen aka IAAS / SAAS

- Eigene Pentests vs bereitgestellte
  - PCI DSS - Scope prüfen !
  - Fragt ob man selbst Pentest macht
  - Stellt einen Anforderungskatalog auf
    - Pflicht Inhalte, Aufbau, Scope, Zyklus, Methoden
- CISO Team / Konzerneinkauf
  - Änderung der Rahmenverträge durchführen
  - Richtlinien müssen auch dort Geltung haben
  - Verstöße melden und als Risiko einwerten lassen
  - Externer Betrieb != Keine Verantwortung mehr
  - Prüfer können hier Picky werden

Pentesting

Security Geraffel

Vorbereitungsphase

- Vorlaufplanung (3 - 6 Monate im Vorfeld)
  - Grobplanung, Anfragen an Pentestfirmen für Platzhalter, etc...
- Onboarding (4 Wochen davor)
  - KickOff mit TAV, Scoping und Out-of-Scope
  - § 202 StGB Klausel erledigen
- Identity Management (2 Wochen davor)
  - Zugänge und Berechtigungen bestellen
- WAF / Firewall (1 Woche davor)
  - Anträge stellen (Request Fulfillment)
- Readiness Check (2-3 Tage davor)
  - Letzte Möglichkeit zu Verschieben oder Abzusagen

Und Action !

- Im Best-Case Szenario läuft alles Reibungslos

- Realität kann sein:
  - Zielumgebung ist Down wegen Fehlkommunikation von “plötzlichen” Updates
  - Die Anwendung crasht durch einen Portscan
  - Kritische Findings treten auf
  - Fragen der Pentester suchen Antworten
  - Plötzliche Bedenken der TAV / Fachbereiche
  - Provider stellt sich quer
  - SNAFU tritt ein

Nachbereitungsphase

- Report Finalisierung
  - Einige Pentest Firmen wollten Anfangs noch ihr Layout verwenden
  - Korrekturlesen - Aber keine Inhaltlichen Änderungen durchführen!
- Abschluss Meeting
  - Klare Findings und produktive Verbesserungsvorschläge gegenüber TAV
  - Miteinander statt Gegeneinander (nix P.A.L.)
- Tracking Sheet
  - Dient der Dokumentation für
    - Anderes internes Rating bei Findings (CISO Team hat Vetorecht)
    - Besprochene Vorgehensweisen
- Problem Tickets
  - Keine Inhalte, nur Verweis auf Finding-ID (Vertraulichkeit)

Sir, we fucked up !

- Ups - Pentest fällt aus
  - Ehrliche und frühzeitige Kommunikation gegenüber Pentest Firmen
  - Immer ein oder zwei alternative Pentest Ziele im Ärmel haben
  - Bei Pentest Bundles Scope Change durchführen und dokumentieren
- Es hagelt Findings
  - TAV direkt einbeziehen mit Hilfestellung durch Pentester
  - Durchziehen bis zum Schluß für möglichst tiefe Testabdeckung
  - Dokumentieren und Eskalieren
- Pwnd
  - Mitigierende Maßnahmen einleiten
  - Prüfen ob weitere Anwendungen betroffen sein können
  - Dokumentieren und Eskalieren

Konsequenzen

- None-Compliance und Sachverhalt Meldungen
  - Auswertung nur 1x im Jahr (Risikoappetit des Konzerns)
- Risikoakzeptanz eine Lösung?
  - Gilt nur Intern
  - Muss detailliert Dokumentiert sein
- Mid Term/Long Term Solution
  - Optimal: Bugfix
  - Realistisch: Mitigierende Maßnahmen
    - IDS / IPS
    - WAF
    - DMZ
    - Firewall
    - SIEM

Möglichkeiten zur Vermeidung

- CI/CD als Lösungsansatz?
  - Einbringung als DevSecOP mit Toolunterstützung bei Eigenentwicklungen
  - Continuous Integration / Continuous Deployment mit Quality Gates
- GRC Control Vorgaben
  - Pentest Control erfüllt, aber mit Auflagen
  - Ziel ist es, Risiken in Monetärer Form (Risikorücklage) zu manifestieren
- BMA Integrieren
  - Entweder die IT betreibt es, oder es existiert nicht (AppControl auf Win10)
  - Auflagen und Backing durch CISO
- Tools vs Orga
  - Nessus, Nexpose, NMAP, OpenVAS Scans im Vorfeld (Zyklisch / Azyklisch)
  - Erstellung konkretisierende Sicherheitsvorgaben, u.a. basierend auf Findings

Vorteile externer Pentest Firmen

- Größere Auswahl an Skillsets
- Flexibler da größere Auswahl an Personen
- Kosten sind planbarer
- Keine Ausfälle wegen
  - Konferenzteilnahmen oder Schulungen
  - wegen Krankheiten
  - Interner Unstimmigkeiten
- Keine Abhängigkeiten zum Auftraggeber
  - Reports und Inhalte werden weniger angezweifelt
  - Zügige Lieferung der Ergebnisse
  - Offene Kommunikation

Nachteile und Kostenfaktoren

- Externe Pentester sind teurer !
  - Man spart aber die folgenden Kostenblöcke:
    - Schulungskosten
    - Konferenzkosten
    - Ausstattungskosten
    - Reisekosten (nicht immer)
- Qualität der Reports und Findings schwankt
  - Prüfen, Feedback geben und Personen aussortieren
  - Offene und ehrliche Kommunikation ist hilfreich und schont Nerven
- Kein Einblick in die internen Abläufe des Auftraggebers
  - Gerade bei komplexeren Systemen eine Herausforderung
  - Vorteil ggfs. !?

Abschluss

Erfahrungen aus dem RL - Intern

- ITIL Fan im Team erzeugt Chaos
  - Nur eine Vorgehensweise im Kopf möglich...
- Vermischen von Inhalten in der Kommunikation
  - Firmen / Inhalte / Scope / Planungs-IDs vermischt
- Projekte welche vor lauter AGIL die Realität vergessen zu beachten
  - Runs alle sechs Wochen und nur wenige Tage für Tests/Pentests geplant
- Externe Entwicklungsfirmen mit Mängeln
  - Unsere Anwendung ist sicher. Sowas gibt kein Anwender ein
  - OWASP ? Steht im Vertrag, aber nie von gehört
- Interner Widerstand
  - Kostet doch eh nur und bringt nichts...
  - Haben Sie nichts besseres zu tun als mir meine Zeit zu stehlen?

Erfahrungen aus dem RL - Extern

- LibreOffice anstatt Microsoft Office
  - Killt so ziemlich jede M$ Word Template Vorlage
  - Wasserzeichen als Bild im Header verankert, anstatt die Office Funktion zu nutzen
- Inkonsistente Reportinhalte
  - Finding vs. Text passen nicht
  - Vermutungen statt PoC
  - Planungs ID wird durch eigenen Mischmasch ersetzt
  - Veraltete Reportvorlage
- Kommunikation
  - Keine Erreichbarkeit weil Kontakt im Urlaub ist
  - Vermischen von Planungs IDs
  - Info über Start nur nach mehrmaligem Nachfragen

Fazit

- Andere Kochen auch nur mit Wasser
- Als Manager bist du ohne Prozesse und Workflows nur am Schwimmen
- Pentests sind kein Selbstzweck
- Gesunde Mischung aus P.A.L. und WIR
- Es benötigt kein eigenes Pentest Team mehr

  Oder

  Kleineres internes Team für Longrunning Pentests, der Rest extern
- CI / CD mit DevSecOps helfen die Findings zu reduzieren (kein Allheilmittel !)
- Tools lösen **keine** Organisatorischen Probleme !
- Kommunikation ist das A und O

Danke für eure Zeit !

Kontakt

Twitter: MrMarco74

Blog: https://www.security-geraffel.de

Threema: HBEHWEMW