NTT Security

Operation IT-Sicherheit: Best Practices zur Minimierung des digitalen Infektionsrisikos

Information Security in Healthcare Conference

Miro Ljubicic
22. Juni 2017

[Miro Ljubicic]-[Public]-[Approved]-v[1.1]

Vorstellung Miro Ljubicic

Seit 2004 in der IT

- 7 Jahre Operations im HR-Umfeld
- 6 Jahre in Secure Operations
- Seit Oktober 2013 bei NTT Security als IT Security Consultant
- Seit März 2017 Teamlead Cyber Defense Switzerland

Schwerpunkte:

- SIEM / Log Management
- Incident Response
- Vulnerability Management
- Security Process Design

Inhalt

Unsere Arbeit glänzt durch Vielfalt…

pixabay.com

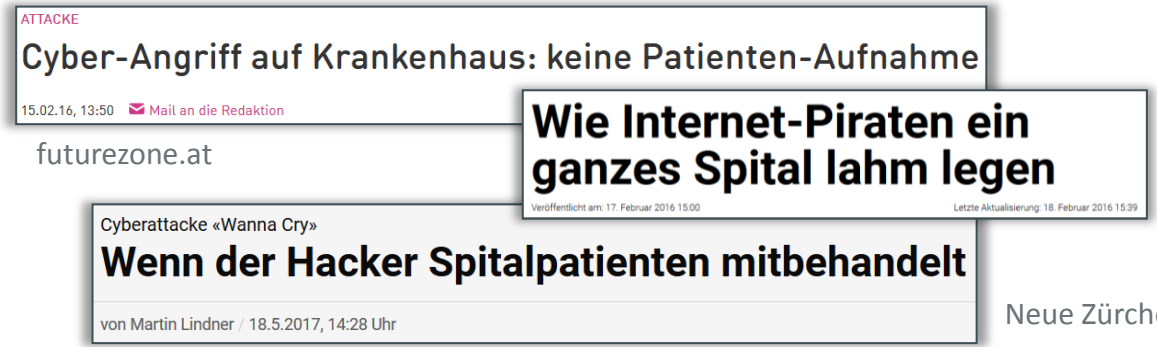
… heute müssen wir uns aber auf ein paar Themen beschränken.

Inhalt

1. Aus der Praxis
2. Alte Herausforderungen…
3. Neue Herausforderungen…
4. Cyber Defense von A bis Z mit NTT Security
5. Fazit

Aus der Praxis

Wir könnten uns jetzt gemeinsam viele Statistiken und Schlagzeilen anschauen…



futurezone.at

medinside.ch

Neue Zürcher Zeitung

… aber ist das wirklich zielführend?

Aus der Praxis

Lassen wir doch unsere Kunden zu Wort kommen…

«Warum brauchen wir Vulnerability Management? Am Ende braucht es doch sowieso einen Patch, und Patch Management machen wir doch schon…»

«Wir wissen eigentlich (noch) gar nicht, was für Systeme wir genau haben…»

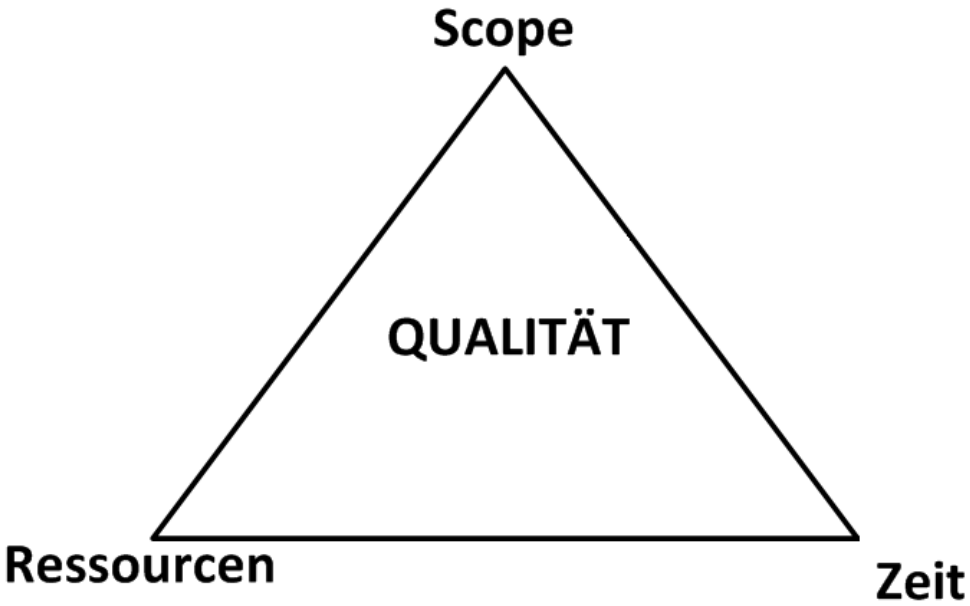
«Der Headcount muss noch bewilligt werden / der nächste Bewerber kommt am Freitag…»

«System / Lösung XYZ ist zertifiziert und darf nicht verändert werden»

«Wieso fehlen uns ausgerechnet diese Logs für diesen Incident?»

«Es muss doch etwas besseres geben, als ständig Systeme wegen Viren neu aufzusetzen…»

Aus der Praxis



Alte Herausforderungen…

… brauchen zeitgemässe Lösungen!

Alte Herausforderungen…

1. Governance, Risk Management, Compliance – Eine Hassliebe

2. Security Monitoring – Zwischen Polizeistaat und Datengrab

Governance, Risk Management, Compliance

Eine Hassliebe

Alte Herausforderungen… Governance, Risk Management, Compliance

Was ist das meistgenutzte Tool für IT-Administration weltweit?

Microsoft® Excel

Was ist auf dem besten Weg, das meistgenutzte Tool für IT-**Security**-Administration weltweit zu werden?

Microsoft® Excel

Alte Herausforderungen… Governance, Risk Management, Compliance

Ist das tatsächlich der Weg, den wir einschlagen sollten?

“Computer says no…”

Wachsende Datenkomplexität lässt sich nur schwer in “Zeile x Spalte” pressen

Moderne Verwaltungstools sind zu mehr fähig als nur CSV-Exports

Automatischer Datenaustausch ist heute kein leeres Versprechen mehr
(API, DXL, STIX/TAXII, OpenIOC)

Alte Herausforderungen… Governance, Risk Management, Compliance

Wie können wir es besser machen?

Zentrales Asset Inventory
(prozessintegriert)

Nutzung von API-Schnittstellen

Zentrales Logging für Statistik, Audit-Evidenz
und Ad-hoc-Reporting (SLA, OLA, KPI…)

Policy Management and Enforcement
(Prozesse für Risikobeurteilung, Vuln.
Management und Incident Response)

Security Monitoring

Zwischen Polizeistaat und Datengrab

Alte Herausforderungen… Security Monitoring

Woran erkennen Sie, dass Sie **zu wenige** Security Events im Monitoring haben?

Genau: Ausgerechnet die Events, die frühzeitig einen Vorfall hätten erkennen lassen oder zumindest bei dessen Analyse geholfen hätten, fehlen!

Woran erkennen Sie aber, dass Sie **zu viele oder unnütze** Security Events im Monitoring haben?

Genau: Meistens gar nicht, ausser es gibt Performance- oder Lizenzprobleme

Alte Herausforderungen… Security Monitoring

Wie können wir es besser machen?

Zweckgebundenes Monitoring
(nur die Bereiche überwachen, für die man auch eine Handhabe hat)

Anomalie-Erkennung

Einbindung von Kontextdaten
(Schwachstellen, High-Risk-Systems, sensitive Netze)

Integration mit Incident Response

Neue Herausforderungen…

… lassen sich mit Erfahrung besser meistern!

Neue Herausforderungen…

1. Advanced Malware / Ransomware – Die “Bösen” können nun auch Crypto

2. Effektives SOC – Gutes Personal wächst nicht auf Bäumen

NTT Security

Advanced Malware / Ransomware

Die “Bösen” können nun auch Crypto

Neue Herausforderungen… Advanced Malware / Ransomware

Mit den traditionellen Schutzmassnahmen verlieren wir das Rennen…

Endpoint AV Lösungen (auf Signaturbasis) werden obsolet

Vernachlässigtes Patching ist einer der Gründe für schwerwiegende Vorfälle

IDS/IPS-Signaturen kommen oft zu spät

Crypto Malware profitiert auch von schneller CPU und SSD

SSL-Verbindungen zu CnC Servern werden die Regel

Netze oft zu flach organisiert (leichtes Spiel für Lateral Movement)

Neue Herausforderungen… Advanced Malware / Ransomware

Wie können wir es besser machen?

Aufbau von Advanced Malware Lösungen
(Perimeter, Email + Endpoint)

Netzwerksegmentierung

Einbezug von Serversystemen in den Scope

Client-Backup-Lösungen und Nutzung von Group-Shares
konsequent umsetzen

Effektives SOC

Gutes Personal wächst nicht auf Bäumen

Neue Herausforderungen… Effektives SOC

Was häufig angetroffen wird:

Secure Operations ist “nur” ein Teil der regulären IT-Operations (oft im Nebenamt)

Fehlende SLAs, OLAs oder sonstige Vorgaben (Security als “best effort”)

Grosser Umfang an Einzellösungen, aber kein schlüssiges Gesamtkonzept
(auch in Beschaffungsfragen)

Vielzahl externer Services verschiedener Anbieter ohne nennenswerte Integration
(Excel als Drehscheibe)

Neue Herausforderungen… Effektives SOC

Wie können wir es besser machen?

Konzentration auf wenige, dafür umfassend agierende Dienstleister

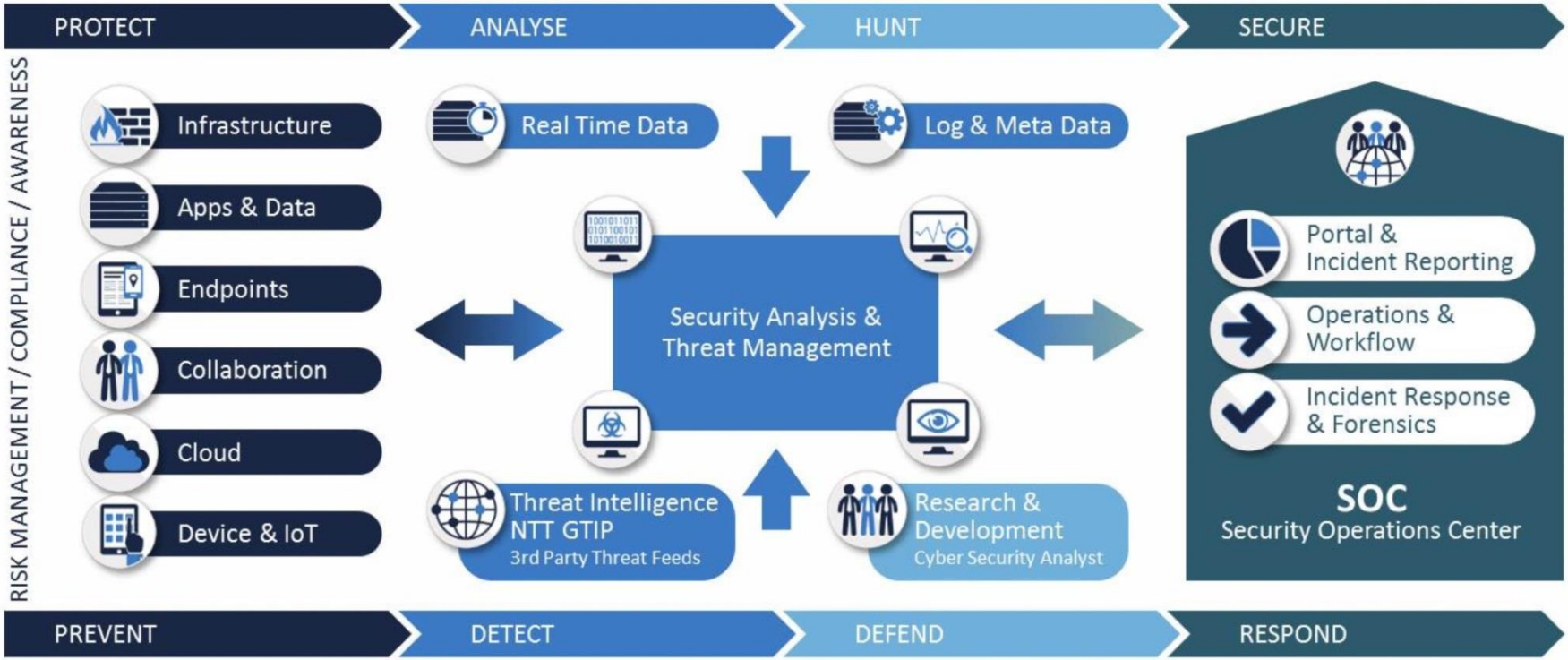
Eigenständiger Security-Betrieb mit genügend Stellenprozenten

Schaffung, Implementierung und Einhaltung von Prozessen, SLAs, OLAs und sonstigen Messkriterien

Integration mit Incident Response

Cyber Defense von A bis Z mit NTT Security

Cyber Defense von A bis Z mit NTT Security



Fazit

Fazit

Hausaufgaben machen…

- **Bekannte Problemstellungen durch etablierte Lösungen rasch angehen**
  - Policies konsolidieren und durchsetzen
  - Zentralisiertes Asset Inventory und Security Monitoring
  - Netzwerksegmentierung und Network Access Control
  - Prozesse prüfen und umsetzen

- **Kapazitäten für neue Herausforderungen schaffen…**
  - Advanced Malware Protection
  - Client Backup and Recovery
  - Aufbau SOC und Incident Response

Fazit

- **Strategische Überlegungen anstellen:**
  - Abwägen zwischen Nischenlösung und Gesamtstrategie
  - Investitionen in wichtige Bereiche, nicht in dringende
  - Wahl geeigneter Dienstleister
  - Auslagerung einzelner Funktionen

Vielen Dank… let’s talk!

Miro Ljubicic
Miro.Ljubicic@NTTSecurity.com