

> Digital Forensic
Readiness – Incident – Compromise
Assessment

- Zertifizierter Forensiker CHFI
- Information Security Officer ISO27000
- EDV Sachverständiger EDV-Systeme

-
- Öffentliche Auftraggeber
 - Unternehmen der freien Wirtschaft
 - Privat Personen
 - Bildungseinrichtungen

- Seit 2010 bei Rednet
- Enterprise Consultant
- System Architekt



- Langjährige Partnerschaft
- Zusammenarbeit seit 2013
- Stetige Erweiterungen der Kompetenzen
- Produkte: Server, Storage, WLAN, Campus IP, DC IP
- Rednet & Huawei bedienen zwei Bundesländer über gewonnen Ausschreibungen



> Der Fall

Unser Kunde:

- Mittelständisches Unternehmen der Konsumgüterindustrie
- Regelmäßige Preise für Design und Innovation seiner Produkte
- Fertigung und Produktion in Deutschland
- Vertriebsbüros weltweit
- Ca. 2000 MA

> Der Fall

Problemstellung:

- Marktbegleiter bringt innerhalb kurzer Zeit auffallend ähnliches Produkt auf den Markt
- Viele Details gleichen sich
- Möglicher Datenabfluss ???

IT- Leiter

- Lässt sich zunächst zum Thema Datenabfluss beraten
- Vertraulichkeit der Untersuchung
- Rücksprache mit der GF

Meeting mit GF /IT / DSB

- Untersuchte Daten dürfen das Unternehmen nicht verlassen
- Untersuchungs-Team zusammenstellen
- Zeitnaher Beginn der Untersuchung
- Einbindung interner Ressourcen

Interne Mitarbeiter

- Datenschutzbeauftragter
- Betriebsrat
- Syndikusanwalt
- IT-Leiter
- Chief Information Security Officer ???

Externe Dienstleister

- Stefan Würth
- Riccardo Witzmann
- Dediziertes Forensic Support Team



> Die Robo Lösung

Komponenten	Konfiguration	Anz	HE	Anwendung	Zusatz
Modular Server	4 * compute node, each with: <ul style="list-style-type: none"> 2 * Intel Xeon Gold 5120 (14-core) 16 * 32GB DDR4 memory 2 * 240GB SSD 	1	2U	Virtualisierung (224 vCPU, 2TB RAM),	8x 10G Ports
Rack Server	2 * Intel Xeon Gold 5122 (4-core) 12 * 64 GB DDR4 memory 2 * 240GB SSD 5 * 1.6 TB SSD	1	1U	Datenbank Server, 768GB RAM	2x 10G Ports
Rack Server	1 * Intel Xeon Silver 4108 (8-core) 3 * 8 GB DDR4 memory 2 * 240GB SSD 4 * 2TB NL-SAS	1	1U	Ingestion Server	2x 10G Ports
Storagesystem	Dual-Controller 64GB Cache & 8x 10G SFP+ 12 * 3.84TB SSD 25 * 2.4TB SAS disks	1	4U	Storage, 100TB Kapazität SSD: R10+1 HLOW = 33,5TiB SAS: R12+1 HLOW = 45.67TiB	4x 10G Ports
Switching	48-port (32 * GE Base-T, 16 * 10GE SFP+)	2	2U	10GE switch (10G service network and 1G manage network)	Port Mirroring möglich
Software	Hypervisor	1	Software	Virtualisierung	
Rack Case Mobil	Abschließbar, Stoßfest	1	12U		

> Ausgangslage

- Nur MA der R&D haben Zugang zu den Konstruktionsdaten
- Alle MA mindestens >10 Jahre im Unternehmen
- Personenkreis beschränkt sich auf ca. 20 MA
- Segmentiertes Netzwerk
- Leasing der Hardware

> Sofortmaßnahmen

Unmittelbare Sicherung der Logs

- Anti-Virus
- Firewall
- Active-Directory
- Netzwerkswitches
- Workstations der R&D
- ...

> Erste Auswertung und Zwischenstand

- Keine Hinweise auf Schadsoftware
- Kein Hinweis auf Datenabfluss
- Virens Scanner und Patchmanagement aktuell
- Kein besonderes Logging (Log Server)
- Keine Mitarbeitervereinbarungen zur PC Benutzung

> Weiteres Vorgehen

- Interview mit MA
- Rechnertausch vor ca. 4 Wochen
- ausgetauschte Rechner wurden aus dem Sperrlager hervorgeholt

> Weiteres Vorgehen

- Aufsetzen einer Sandbox (VM)
- Malware Analyse auf den ausgetauschten Rechnern
- Analyse der Festplatten durch forensische Sicherung
- Isolation der Malware

- Proxy-Logs
- Virens Scanner der ausgetauschten PC:
 - > Teilinfektionen die nicht bereinigt werden konnten
- DLL ausgetauscht

- Per Mail an 5 verschiedene MA über einen Zeitraum von 5 Monaten
- Privilegien-Ausweitung
- Unbekanntes Konto auf dem AD

- Erstellung einer Timeline
- Infektion durch Malware vor 5 Monaten
- Zugriff auf das PDM-System (RDP)
- Gezielte Suche nach Neuentwicklungen
- Nicht alle Spuren konnten vollständig rekonstruiert werden

- Zugriff erfolgte vorwiegend über eine Person (Teilkonstrukteur)
- Password Dumper gefunden
- Zugriff auf verschiedene Systeme konnte nachgewiesen werden

> Probleme bei der Untersuchung

- Keine Regelung für den Email Zugriff
- Schwache Regelung für Internetbenutzung
- Fehlerhafte Netzwerkübersicht
- Bereitstellung von Log-Files

> Weitere Maßnahmen

- Kompletter Scan der IT-Infrastruktur
- Härtung verschiedener Systeme
- Sensibilisierung der MA
- Erstellung von Unternehmensrichtlinien

> Weitere Maßnahmen

- Schwachstellenmanagement etabliert
- Eskalationwege beschrieben
- Funktion CISO eingeführt
- Log Server installiert

> Zusammenfassung

Umfangreiche Untersuchung ein Zusammenspiel von:

- mangelnder „Forensik Readyness“
- „Incident Response“
- „Compromissed Assesment“

- Gerichtsverwertbare Aufarbeitung der Beweislage
- die GF prüft weitere Schritte
- IT Sicherheit steht nun auf der Agenda

- Analyse mehrere GB Daten auf Log Files
- Analyse von 2*15 Workstation
- Entwicklung eines mobilen Rechenzentrums

■ Haben Sie Fragen ?

forensys.it
Stefan Würth
An der alten Schule 5
51709 Marienheide
Tel. 0160 / 2797814
kontakt@forensys.it
www.forensys.it

Rednet AG
Riccardo Witzmann
Carl-von-Linde-Straße 12
55129 Mainz
Tel. 06131 / 250 62-0
info@rednet.ag
www.rednet.ag



> VIELEN DANK
für Ihre Aufmerksamkeit.

REDNET AG | IT-AUSSTATTER

für Behörden und Bildungseinrichtungen

Carl-von-Linde-Straße 12 | 55129 Mainz

T 0 61 31 . 250 62-0 | F 0 61 31 . 250 62-199

info@rednet.ag | rednet.ag | hochschule.rednet.ag

