

Wolfgang Straßer
Geschäftsführer
@-yet GmbH



Forensik in der Praxis

Firmenportrait

- Juni 2002 gegründet
- Sitz: Leichlingen/Rheinland

- IT-Strategie- und Technologieberatung
 - kein HW- oder SW-Vertrieb

- Beratungsschwerpunkte
 - IT-Risikomanagement
 - IT-Outsourcing

- Zielgruppe:
 - Mittelständische bis große Organisationen

IT und Risikomanagement

Aufgaben von IT Risikomanagement:

- Schutz vor Verlust von
 - Know-how und
 - Wertschöpfung

- Schutz vor Risiken, die sich
 - vertraglich
 - gesetzlichaus der IT ergeben können.

IT und Risikomanagement

Elemente von IT-Risikomanagement

- Business Continuity
- Business Security
- Business Compliance

- IT-Forensik

Forensik

- Firmennetzwerke sind komplexe Gebilde.
 - es ist nahezu unmöglich, keine Spuren zu hinterlassen
 - es ist ebenfalls möglich, alles zu fälschen.
- Die Kunst ist es, echte Spuren von falschen zu unterscheiden
- Nicht alle Informationen werden anerkannt.
- Der kleinste Fehler kann die gewonnenen Informationen in ihrer Verwertbarkeit beeinträchtigen
 - leicht kann man unbeabsichtigt Spuren zerstören

➤ Der Fall

Ausgangslage APT

- Kunde:
 - Internationaler Konzern – im DAX gelistet
 - innovativen Entwicklungen/ Know-How getrieben
 - Umgang mit Gefahrgüter
 - mehrere zig-tausende Mitarbeiter

- Mail von Sicherheitsfirma im Ausland
 - Malware mit „Zugangsdaten“ des Kunden gefunden
 - Benutzername passt zu einem „Administrator“
 - Proxy-IP fest einprogrammiert

Reaktion: Ja? Nein? Wie?

Was ist
tatsächlich
passiert?

Kann ich es mir
Leisten nicht zu
reagieren?

Unlautere
Akquise?
Erpressung?

Inhouse-
Ermittlungen vs.
unabhängige
Experten?

Wieviel kostet es,
wenn da nichts
war?

Was ist betroffen?
Kommunikation?

Wem kann
man trauen?

Ist da was
dran?

Kontakt-Aufnahme Forensik Team-@-yet



➤ Empfehlungen:

- Sofortige Reaktion
→ Geschwindigkeit ist essentiell
- Sammeln der Fakten
- Erste Analyse um Problem zu bewerten
- Anfrage weiterer Informationen bei Sicherheitsfirma
- Einschalten des Verfassungsschutz (Spionage-Abwehr)



Erstes Meeting beim Kunden (2. Tag)

Das Team:

- Konzern-Sicherheit
- IT-Sicherheit (CISO)
- Konzern-Legal (Datenschutz+Jurist)
- **IT-Infrastruktur und -Betrieb**
 -  Interessenskonflikt:
 - Vorgesetzter des Administrators
 - Verantwortlich für aktuelle IT-Lage
- **IT-Administrator**
 -  Interessenskonflikt:
 - Kollege des betroffenen Administrators
- Verfassungsschutz
 - (Initial und später punktuelle Unterstützung)
- @-yet GmbH

Erste Informationen

- Kopie der Schadsoftware
 - Ausl. Sicherheitsfirma kooperiert (ohne nach Geld zu fragen)
- Malware: C&C-Server mit Kundennamen im Domänennamen
 - Internet-Suche „Kundennamen“ + Malware
 - Sample konnte aus Malware-Datenbank bezogen werden
- Sicherung Logs (umgehende Sicherung empfohlen)
 - Anti-Virus
 - Firewall
 - VPN
 - Active-Directory
 - ...

Zwischenstand - Ausgangslage

- Noch keine Hinweise im Konzern-Netz
- 2 unterschiedliche Schadcodes identifiziert
 - Evtl. unabhängig
 - Keines wurde auf Kundensystemen gefunden
 - Antivirus-Erkennung: 0/54 auf Virustotal
- Es hat auf jeden Fall einen Sicherheitsvorfall gegeben
 - Benutzername und Proxy sind nach Außen gelangt
 - rechtfertigt Ermittlungen

Vorgehen

- Mehrere Tracks:
 - Malware-Analyse
 - Merkmale infizierter Systeme identifizieren
 - Tathergang aufklären
 - Sichtung Logs
 - Allgemeine Suche nach Spuren
 - Gezielte Suche nach aus Malware identifizierten Merkmalen
 - Analyse Festplatten identifizierter Systeme
(forensische Sicherung der Platten)
 - Prüfen von „Kernkomponenten“ auf Manipulation
 - Background-Informationen
(Domänen C&C-Server, Domänen-Inhaber, ...)

Nachweis von Infektionen

- Proxy-Logs
 - Täglich Gigabytes – Kommunikation mit bekanntem C&C-Server geblockt, soweit die Logs zurückgehen
 - Ca. 15 Rechner betroffen
(mehrere Admin-Rechner/ Server)

- Virens Scanner
 - Teilweise Infektionen erkannt, die nicht bereinigt werden konnten

- Rechner Administrator (keine Infektion)
 - Nutzung erst seit ca. 1 Monat
 - davor anderes Notebook, alte Platte existiert noch

Analyse der Notebooks(1)

- Identifikation der für Datenverkehr verantwortlichen Malware
- Live-Analyse von Kopien in virtuellen Umgebungen
- Time-Line
 - Priorität um bekannte Zeitpunkte
 - Zeit von Infektion bis jetzt
 - Zeit vor Infektion

Analyse der Notebooks(2)

- Analyse gelöschte Dateien
- Analyse Logs
- Aufstellen von Vermutungen aus Analyse-Daten (Nachweis erfolgt später)
- Analyse der Historie für den Infektionszeitpunkt
- Zurückverfolgen des Infektionswegs

Ergebnisse – Notebook-Analyse(1)

- Infektion bereits vor 3 Monaten
- Infektionen erfolgen in sehr kurzem Abstand
- Zustand der Spuren sehr unterschiedlich
 - Teilweise nur punktuell rekonstruierbar
- Manipulation lokaler Zertifikats und Schlüssel-Speicher
- Austausch von Windows-DLLs gegen alte Originale

Ergebnisse – Notebook-Analyse(2)

- Downgrade von Sicherheitsmaßnahmen
- Auf den Systemen wurden zahlreiche Tools aufgebracht
 - Standard Administrationstools
 - Netzwerk-Scanner (Ports / Fileshares)
 - Password-Dumper (RAM/ Domäne)
- Zugriff per Remote-Desktop auf diverse Systeme

Ergebnisse – das Smartphone

- Jailbreak-Tool für Android-Smartphone auf Administrator-Notebook
 - Zeitstempel passt zum Angriff
 - Administrator hat sein privates Smartphone mit Firmennotebook verbunden
 - Angebl. kein bewusstes Rooten des Gerätes
 - Das Geräte wurde nicht zur Analyse bereitgestellt (Privatgerät)
 - Laut Synchronisationslog besteht der Verdacht, dass eine Spy-App installiert wurde

Angriffsweg

- Gezielte Email an ca. 20 ausgewählte Personen
 - Waterhole/Spearphishing
- Drive-By-Download auf „vertrauenswürdiger“ Webseite (Schadsoftware wenige Minuten vor Erstinfektion hochgeladen)
- Installation Malware (Analyse Systemkonfiguration, Download Malware)
- Kontroll-Malware (Remote-Shell / Upload /Download)
- Upload von Tools
- Interaktive Zugriffe

Zwischenbilanz

- Passwörter mehrerer Administratoren kompromittiert
- 3 Monate voller Zugriff
- Systemsicherheit gesenkt
- Passwort-Dumper gefunden
- Modifiziertes Mimikatz gefunden (Golden-Ticket-Funktion)
- Komplette Netz-Übersichten
- Zugriff auf mehrere zentrale Server nachweisbar
- Verdacht auf Infektion von privaten Smartphone

Reaktion des Kunden

Kunde schließt entgegen jeglicher Anzeichen folgende Zugriffe, auf Grund der theoretischen Folgen aus:

- Active-Directory-Passwörter
- Produktion
- Gefahrgüter

Einer Überprüfung der Systeme wird auf drängen @-yet zugestimmt.

Ergebnis der Überprüfung

- Es wurden in allen kritischen Systemen Schwachstellen identifiziert, über die ein Zugriff möglich gewesen wäre
- Auf einzelnen Systemen aller 3 Sicherheitsbereiche wurden tatsächliche Anhaltspunkte für einen nicht autorisierten Remote-Zugriff identifiziert
- Bei anderen Systemen waren auf Grund mangelnder Spuren keine Analysen mehr möglich

Erschwernisse (1)

- Logs wurden nicht oder erst spät geliefert
 - Logs nur vereinzelt verfügbar / nach Tagen
 - Teilweise nur wenige Minuten

- Es stehen keine Austausch-PCs zur Verfügung
 - Infizierte Rechner bleiben noch ca. 1 Woche in Betrieb
 - Benutzer werden über Infektion nicht informiert
 - Infizierte Platten wurden nach dem Anfertigen von Kopien ohne Bereinigung trotz Warnung an die Mitarbeiter zurückgegeben

- Falsche PCs werden geliefert

- Alternative Internet-Zugänge wurden verschwiegen

Erschwernisse (2)

- Altes Notebook des Administrators
 - Administrator wird informiert
 - 2 Stunden später wird die alte Festplatte geliefertForensische Rekonstruktion:
Letzte Aktion: 10 Minuten vor Übergabe wurden Programme, Filme, Serien und Musik gelöscht
- IT-Verantwortlicher erschwert Analysen, um ggf. Versäumnisse zu vertuschen
- Keine funktionierende IS-Organisation
- Kennwort-Änderungen waren systematisch (neues Kennwort ableitbar)

Vorwürfe

IT-Verantwortlicher unterstellt Inkompetenz, fehlende Warnungen beim Weiterbetrieb infizierter Systeme

- Sämtliche Verzögerungen, Aktionen, Warnungen und Zwischenstände sind dokumentiert
- Die Vorgehensweise und Ergebnisse konnten auf Grund lückenloser Dokumentation durch unabhängige Sachverständige nachvollzogen werden



Bei Forensiken wird man schnell von der Rolle des Analysten/Geschädigten zum Angeklagten gemacht. Daher ist lückenlos dokumentieren Pflicht.

Herzlichen Dank für Ihre
Aufmerksamkeit!

Ihre Fragen bitte...

Wolfgang Straßer
wolfgang.strasser@add-yet.de

