THE PENTEST EXPERTS.

In diesem Newsletter erwarten Sie folgende Inhalte:

Sehr geehrte Kunden,
liebe Geschäftspartner,
Freunde und Bekannte,

Hacking verursacht nicht nur einen immensen wirtschaftlichen Schaden, sondern auch eine nicht zu unterschätzende Rufschädigung. Allein im Dezember 2014 ereigneten sich vier prekäre Vorfälle. Zunächst wurde bekannt, dass Angreifer E-Mails von Mitarbeitern, Drehbücher und sogar ganze Filme von Sony Pictures Entertainment kopiert und teilweise veröffentlicht hatten. Das Ziel bestand darin, den Konzern zu erpressen und die Veröffentlichung des nordkoreakritischen Satirefilms „The Interview“ zu verhindern. Dem US-amerikanischen Büromaterialhändler Staples waren kurz zuvor mehr als eine Million Kreditkartendaten seiner Kunden gestohlen worden. Wiederum wenige Tage später traf es Sony erneut: Neben Microsofts X-Box wurde auch Sonys Playstation Network angegriffen, sodass während der Weihnachtsfeiertage die gesamten Spieledienste nicht mehr verfügbar waren. Besonders spannend bei diesem Angriff war, dass sowohl Angriffsart als auch Zeitpunkt in einem Blog vorab öffentlich angekündigt wurden. Das zeigt die Dreistigkeit des Täters und die Machtlosigkeit selbst großer Konzerne, sich gegen derartige lastbasierte Angriffe zur Wehr zu setzen. Zuletzt wurde der Trojaner „Regin“ auf Rechnern des Kanzleramts gefunden, dessen Autorschaft der NSA zugeschrieben wurde. Angesichts dieser Ereignisse stellt sich die Frage: Wie hoch sind eigentlich die jährlichen Schäden in Deutschland?

Ein Autobesitzer bemerkt, wenn sein Wagen gestohlen wird. Wenn Daten geklaut werden, merkt der Geschädigte davon in der Regel nichts: Nicht selten finden meine Experten bei DFIR-Projekten vor langer Zeit installierte digitale Hintertüren, die es ermöglichen, dass sich Hacker über Jahre hinweg völlig unbemerkt in Unternehmensnetzwerken „tummeln“.

Natürlich wird auch eine Vielzahl von Angriffen entdeckt. Primäres Ziel der geschädigten Unternehmen ist es dann, die „Brückenköpfe“ zu zerstören, die der Täter in der eigenen IT gebaut hat, und den drohenden Imageschaden abzuwenden. Sollten erfolgreiche Hackeraktivitäten bekannt werden, muss der Incident sowohl nach außen hin als auch intern geheim gehalten werden.

Bei Hackern überwiegen ebenfalls die Gründe, ihre Attacken nicht publik zu machen, denn sie wollen ungestört agieren können. Da viele Angriffe gut gemacht sind, gelangen sie nur in den seltensten Fällen an die Öffentlichkeit – und wenn doch, dann erfolgt dies im Sinne der Täter, wie der Fall Sony zeigt. Uns sollte also klar sein, dass wir durch die Presse nur die Spitze des Eisbergs zu sehen bekommen.

Wenn Sie selbst nicht Opfer eines Angriffs werden wollen, rufen Sie mich an!

Herzliche Grüße,
Ihr Sebastian Schreiber

Aktuelle Events

10.03.15	LH Sicherheitsforen Dr. Walter GmbH, Siegburg
11.03.15	LH AnwaltService GmbH, Stuttgart
16.-20.03.15	Mehrere LHs auf der CeBIT 2015
17./18.03. & 14./15.04.15	Seminarleitung „Hackerangriffe auf Stadtwerke“, Frankfurt & Düsseldorf

Detaillierte Informationen zu diesen Veranstaltungen finden Sie auf unserer Homepage www.syss.de.

Aktuelle Schulungen

Hacking I:
09. - 10.03.15
04. - 05.05.15

Hacking II:
11. - 12.03.15
06. - 07.05.15

Windows-Angriffe:
24. - 26.03.15
09. - 11.06.15

Mobile Device:
14. - 15.04.15

IT-Forensik:
21. - 23.04.15

Exploits:
28. - 29.04.15

VoIP
12. - 13.05.15

WLAN:
19. - 20.05.15

IT-Recht:
22.05.15

Incident Response:
23. - 25.06.15

Bei Teilnahmewunsch oder Fragen wenden Sie sich bitte an info@syss.de.

Sollten Sie den Newsletter nicht beziehen wollen, dann teilen Sie uns dies bitte unter newsletter@syss.de mit. Wir werden Sie dann umgehend aus dem Verteiler entfernen.

Impressum:
SySS GmbH · Wohlboldstraße 8 · 72072 Tübingen · Tel. +49 (0)7071 407856-0 · E-Mail: info@syss.de · http://www.syss.de · Geschäftsführer: Diplom-Inform. Sebastian Schreiber
Verantwortlich für Inhalt: Marcus Bauer

THE PENTEST EXPERTS.

Das Auslesen von Memory-Dumps bei Incident-Response

von Christoph Ritter

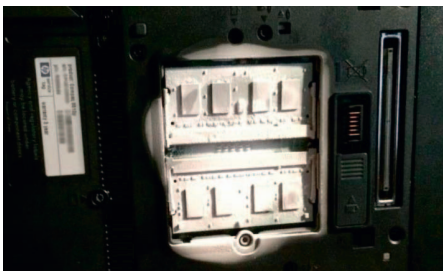
Bei akuten Sicherheitsvorfällen gibt es so manche Vorgehensweise. Eine Möglichkeit besteht im Auslesen des Memory-Dumps. Bei einem Memory-Dump handelt es sich um ein Abbild des Arbeitsspeichers eines Systems. Dieses bietet im Fall einer Incident Response zum einen eine Vielzahl von Informationen und zum anderen den wesentlichen Vorteil, dass im Dump volatile Daten enthalten sind, die bei einer alleinigen forensischen Analyse der Festplatte des Systems nicht existieren. Somit können Analysen, welche sonst nur bei einer Live-Forensik möglich sind, durch die Analyse eines Memory-Dumps auch post mortem durchgeführt werden.

Ein Memory-Dump kann beispielsweise folgende Daten enthalten:

- Schlüssel von geöffneten verschlüsselten Dateien
- Unverschlüsselte Daten, welche auf der Festplatte verschlüsselt abgelegt sind
- Prozessinformationen
- Geöffnete Netzwerkverbindungen
- Angemeldete Benutzer und deren Login-Daten
- In-Memory-Malware
- Nicht gespeicherte Dateien

Damit die Erstellung eines Memory-Dumps zielführend erfolgen kann, ist es essentiell, dass ein betroffenes System nach dem Incident nicht ausgeschaltet wird. Da die Daten im Arbeitsspeicher flüchtig sind und im Normalfall nach wenigen Sekunden verloren gehen, wenn die Stromzufuhr zu dem System unterbrochen wird, sollte bei Sicherheitsvorfällen das System maximal vom Netzwerk getrennt, aber nicht ausgeschaltet werden.

Bei der Erstellung der Dumps werden je nach Szenario verschiedene Methoden eingesetzt. Neben der Möglichkeit, im laufenden Betrieb ein Extrahierungsprogramm im User-Kontext auszuführen, gibt es die Methode einer sogenannten „Cold-Boot-Attack". Dabei kühlt der Forensiker den Arbeitsspeicher auf eine möglichst tiefe Temperatur (-30°C bis -45°C) herunter. Auf der Abbildung ist ein Notebook zu sehen, bei dem gerade ein solcher Angriff durchgeführt wird. Danach wird das System „hart" ausgeschaltet und der Arbeitsspeicher in ein externes System eingebaut und dort ausgelesen. Durch die starke Kühlung des Arbeitsspeichers gehen die Daten trotz der Trennung der Stromzufuhr nicht verloren. Ziel dieses Verfahrens ist es, den Originalzustand des Systems nicht zu verändern und eine Vielzahl von Anti-Memory-Forensik-Techniken auszuhebeln.



Gekühlte Arbeitsspeichermodule
Quelle: Christoph Ritter

Generell muss bei forensischen Untersuchungen auf Datenschutz geachtet werden. Falls es sich bei dem zu sichernden System um ein System im Unternehmensumfeld handelt, auf dem die private Nutzung gestattet ist, muss unter anderem auch die Erlaubnis der betroffenen Benutzer für die Untersuchung eingeholt werden. Bei der Erstellung von Dumps ist es weder sinnvoll noch in den meisten Fällen möglich, Speicherinhalte, die private Daten enthalten, von der Analyse auszuklammern. Damit ein Dump auch vor Gericht als Beweismittel verwendet werden kann, sollte darauf geachtet werden, das Vier-Augen-Prinzip einzuhalten und eine Prüfsumme, eine lückenlose Dokumentation sowie eine Sicherungskopie zu erstellen.

Auch bei der Analyse von Malware zeigt sich, dass die reine Untersuchung eines Festplattenabbildes (Festplatten-Dump), wie es in der Forensik üblich ist, oft nicht ausreicht. So gibt es Arten von Malware, die auf der Festplatte nicht weiter bestehen, sondern lediglich im Arbeitsspeicher gehalten werden. Wurde von einem solchen System ein Memory-Dump erstellt, so kann die Malware aus dem Dump extrahiert und analysiert werden. Kommuniziert die Malware über das Netzwerk, so kann aus dem Dump unter Umständen entnommen werden, wann und mit welchem System die Malware in Verbindung gestanden hat. Somit ist es mitunter möglich, aufschlussreiche Informationen über den Urheber der Malware zu bekommen, ihn eventuell ausfindig und unschädlich zu machen sowie ihn zur Rechenschaft zu ziehen.