Smart Security

Moderner Malware den Kampf ansagen

White Paper

WatchGuard® Technologies, Inc.
April 2014

Patches, Signaturen und das Hamsterrad der IT-Sicherheit

2003 brachte der Computerwurm "SQL Slammer" den Internet-Datenverkehr in vielen Teilen der Welt für mehrere Stunden zum Erliegen.[1] Hierfür wurde eine bekannte Sicherheitslücke der Microsoft SQL-Datenbank, für die Microsoft sechs Monate zuvor ein Patch veröffentlicht hatte, gezielt ausgenutzt. Ausschlaggebend für den zweifelhaften Erfolg und die schnelle Verbreitung von “SQL Slammer” waren dessen geringe Größe sowie die Fähigkeit, sich umgehend zu replizieren, um nach neuen Angriffszielen Ausschau zu halten.

In den darauf folgenden Jahren haben IT-Anbieter auf solche Bedrohungen entsprechend reagiert. Microsoft veröffentlicht inzwischen jeden Monat eine Reihe von Updates, um in der Software entdeckte Schwachstellen zu schließen. Adobe folgt diesem Beispiel und gibt am gleichen "Patch Tuesday" seine sicherheitsrelevanten Aktualisierungen bekannt. Und auch Cisco stellt einmal pro Quartal wichtige Security-Updates vor. Daher sollten IT-Administratoren ihre Systeme regelmäßig aktualisieren, um hinsichtlich potenzieller Sicherheitslücken in der jeweiligen Software auf dem neuesten Stand zu bleiben.

Darüber hinaus bieten Intrusion Prevention Systeme (IPS), die über sogenannte Deep Packet Inspection nach bekannten Mustern für das Ausnutzen von Sicherheitslücken suchen, zusätzlichen Schutz. Antiviren-Programme blockieren Schadsoftware bzw. stellen diese unter Quarantäne. Regularien wie PCI DSS sorgen dafür, dass Unternehmen ihre Antiviren-Software hinsichtlich verwendeter Signaturen aktuell halten. Ein zentrales Management gewährleistet, dass alle Nutzer auf ihren Desktops, Laptops oder mobilen Android-basierten Geräten über den aktuellsten Virenschutz verfügen. Dennoch reichen all diese Vorkehrungen nicht aus, wie auf den nachfolgenden Seiten gezeigt wird.

”Zero Day” heißt das neue Schlachtfeld

Im Bereich der Biomedizin haben Forscher und Ärzte längst verstanden, dass Mikroben und Bakterien sich im Laufe der Zeit weiterentwickeln und immer widerstandsfähiger gegenüber Antibiotika werden. Daher gilt es, stets neue und stärkere Medikamente zur Abwehr zu entwickeln. In der Welt der Informationssicherheit ist dies nicht anders. Es gibt regelmäßig neue Auswüchse von Malware, die gegenüber konventionellen Abwehrmechanismen resistent sind. Auch Angreifer folgen der Evolution und gehen schlauer zu Werke.

Abbildung 1: APT haben Geduld. Es werden verschiedenste Wege gesucht und Angriffe nicht sofort umgesetzt, um größtmöglichen Schaden anzurichten.

[1] http://en.wikipedia.org/wiki/SQL_Slammer

Moderne Malware nutzt fortschrittliche Techniken wie verschlüsselte Kommunikationskanäle, Rootkits auf Kernel-Ebene und andere ausgeklügelte Ausweichmöglichkeiten, um Abwehrmechanismen im Netzwerk zu überwinden. Zudem fokussieren sich entsprechende Angriffe häufig auf Zero-Day-Schwachstellen – also Sicherheitslücken, für die noch kein Patch verfügbar ist und keine Signatur geschrieben wurde. Im Jahr 2012 dokumentierte das WatchGuard LiveSecurity®-Team insgesamt vier solcher Vorfälle. 2013 stieg die Anzahl der von den WatchGuard-Experten registrierten Zero-Day-Attacken bereits auf 13 an.[2]

Neue Malware ist äußerst hartnäckig und darauf ausgelegt, sich festzusetzen. Sie arbeitet diskret und verbirgt ihre Kommunikation sorgfältig – um so lange wie möglich im Netzwerk des Opfers zu überleben. Dazu räumt sie gründlich hinter sich auf, löscht Protokolle, verwendet starke Verschlüsselung und kommuniziert mit dem Controller nur über unscheinbare, nebulöse Meldungsfetzen.

Viele Angriffe basieren inzwischen auf der Kombination verschiedenster Techniken. Je organisierter, qualifizierter, motivierter und finanziell abgesicherter die Angreifer, desto größer die Gefahr: Die Attackierenden haben sehr konkrete Erwartungen und Ziele – meist geht es darum, aus dem Diebstahl von Kreditkartendaten und anderen wertvollen Account-Informationen finanziellen Gewinn zu schlagen.

All diese neuen, fortschrittlichen Formen von Malware werden unter dem Oberbegriff “Advanced Persistent Threats” (APT) zusammengefasst. Abbildung 2 zeigt eine Chronologie der bedeutendsten Zwischenfälle der letzten Jahre, die sich auf APT zurückzuführen lassen.

Während Stuxnet und Duqu die Datenspionage und Manipulation auf Staatsebene zum Ziel hatten, sind heutige Angriffe eher auf finanziellen Gewinn ausgelegt. Ins Zentrum des Interesses rücken in diesem Zusammenhang nicht nur große Konzerne, sondern auch immer häufiger kleine und mittlere Betriebe, regierungsnahe Organisationen sowie industrielle Anwendungen.

Die Folgen solcher Übergriffe sollten keinesfalls unterschätzt werden. So berichtet das Wirtschaftmagazin

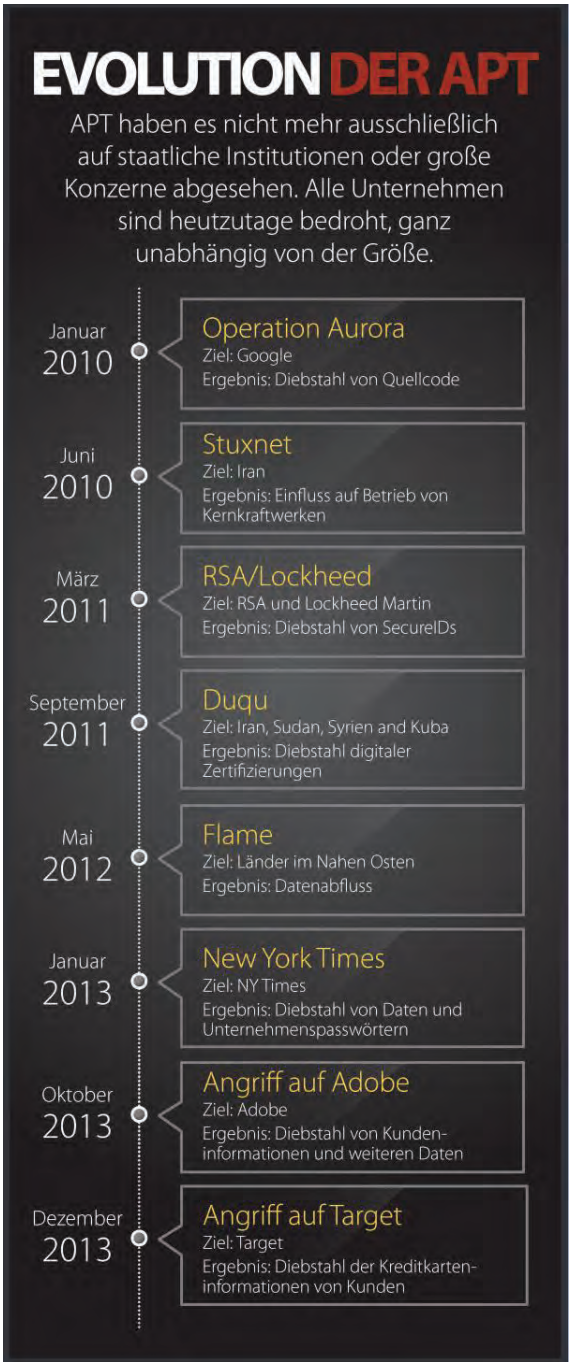

Abbildung 2: Evolution der APT von 2010 bis 2013

[2] http://watchguardsecuritycenter.com

Forbes, dass die Umsätze beim großen US-Einzelhändler Target im 4. Quartal 2013 –insbesondere aufgrund der weitreichenden Berichterstattung zum Verlust der Kundendaten – um fast 50 Prozent eingebrochen sind.[3] Der Aktienkurs fiel um neun Prozent, der CIO hat das Unternehmen inzwischen verlassen. Fünf bis zehn Prozent der Kunden geben an, dass sie nie wieder bei Target einkaufen werden.[4]

Abwehrstrategien auf dem Vormarsch

Das Schreiben von Signaturen verliert an Bedeutung. Bei 88 Prozent der entdeckten Malware handelt es sich um eine Variante bestehender Malware.

Der Kampf gegen Schad-Code gleicht einem Wettrüsten. Sobald neue Verfahren zum Aufspüren der Bedrohungen vorgestellt werden, setzen die Angreifer wiederum alles daran, diese schnellstmöglich zu umgehen. Traditionelle Anbieter von Antiviren-Software beschäftigen Entwickler, um einzelnen Dateien zu analysieren. Sie überwachen das Ausführen unbekannter Programme in abgesicherten Umgebungen oder nutzen Tools wie Anubis, um Dateien zu überprüfen. Verdächtige Aktivitäten oder Verhaltensweisen, die auf einen Virus hindeuten könnten, werden im Zuge dessen angezeigt. Das Schreiben von Malware-Signaturen lohnt sich allerdings kaum noch. Denn die Wahrscheinlichkeit, dass es sich bei neuen Schadprogrammen um Variationen bestehender Malware handelt, bei der klassische Identifikationstechniken an ihre Grenzen stoßen, liegt inzwischen bei 88 Prozent.

Heutzutage haben sich Sandbox-Lösungen im Rahmen der Malware-Erkennung etabliert. Der jeweilige Code wird in der Sandbox ausgeführt und dynamisch analysiert – dies erfolgt automatisiert und ohne weitere Kontrolle durch die IT-Verantwortlichen. Aus diesem Grund versuchen Angreifer alles mögliche, um sicherzugehen, dass ihre Programme in solch einer automatisierten Testumgebung keinerlei Auffälligkeiten zeigen. So werden beim Ausführen von Malware bereits im Vorfeld die Weichen gestellt:

- **Überprüfung hinsichtlich des Einsatzes einer virtuellen Maschine**
- **Abfrage bekannter Windows-Registry-Schlüssel**, die auf eine bestimmte Sandbox hinweisen
- **Einnahme eines Ruhezustands** bis die Analyse der Sandbox zeitlich abgelaufen ist

Darauf haben wiederum die Anbieter von Sicherheitssoftware reagiert und ihren Systemen zusätzliche Intelligenz eingehaucht. Im Zuge von Malware-Abfragen wird zum Beispiel hinsichtlich bekannter Schlüssel geprüft. Zudem können Programme aus ihrem vermeintlichen Schlaf geweckt und somit gegebenfalls als Malware identifiziert werden. Nichtsdestotrotz sind all diese Ansätze nach wie vor reaktiv. Systeme zur Malware-Analyse müssen bei jedem neuen Trick manuell aktualisiert werden. Solange das Update der Sandbox nicht erfolgt, kann der jeweilige Angreifer mit seiner Zero-Day-Taktik punkten.

[3] http://www.forbes.com/sites/maggiemcgrath/2014/02/26/target-profit-falls-46-on-credit-card-breach-and-says-the-hits-could-keep-on-coming/
[4] http://www.usatoday.com/story/money/business/2014/03/11/target-customer-traffic/6262059/

Vollständige Systememulation als Mittel der Wahl

Heutzutage basieren die meisten Sandbox-Implementierungen auf einer virtuellen Umgebung mit dem entsprechenden Gastbetriebssystem. Kernproblem bei solchen virtuellen Sandbox-Szenarios ist die mangelde Transparenz: Es fehlen schlicht und ergreifend Einblicke zur Ausführung von Malware-Programmen. Die Sandbox sollte jedoch so viel wie möglich über das Verhalten der Malware herausfinden, ohne dabei selbst vom Angreifer erkannt zu werden. Denn sobald die Malware vom Einsatz der Sandbox weiß, wird sie ihr Verhalten ändern.

So können moderne Schadprogramme beispielsweise ihre Aktivität nicht nur vorübergehend einstellen, sondern sind auch in der Lage, harmlose Regsamkeit vorzutäuschen. Die wahre Bedrohung lässt sich oftmals nicht identifizieren, da aus Sicht des Analysesystems alles normal erscheint. Daher kommt es darauf an, einzelne Vorgänge im Detail zu hinterfragen.

Zudem fokussieren auf Virtualisierung beruhende Sandbox-Lösungen System- bzw. Windows-API-Aufrufe auf Anwenderebene. Erfasst werden alle Interaktionen zwischen dem Programm und seiner Umgebung (beispielsweise wann Dateien gelesen, Registrierungsschlüssel geschrieben oder Netzwerkaktivitäten ausgelöst werden). Die Sandbox ist jedoch blind gegenüber allem, was zwischen den Systemaufrufen passiert. Dieser weiße Fleck wird zum Ziel der Angreifer.

Entsprechende Lösungsansätze müssen also intelligenter werden. Hier kommen Emulatoren ins Spiel. Gemeint ist damit Software, die die Funktionalität von einem anderen Programm oder einer Hardware simuliert. Da der Emulator verschiedenste Funtionalitäten software-seitig integriert, ergibt sich nicht nur große Flexibilität. Die Emulation des Betriebssystems ermöglicht auch ein hohes Maß an Transparenz hinsichtlich des Malware-Verhaltens. Dennoch können diese Emulatoren nicht jeden Anruf im Betriebssystem replizieren. Sie konzentrieren sich in der Regel auf bestimmte Teilfunktionalitäten. Leider ist dies exakt die Lücke, die fortschrittliche Malware erkennt und ausnutzt.

Eine vollständige Systememulation – bei der der Emulator auch die physische Hardware (einschließlich CPU und Speicher) simuliert, bietet den höchsten Grad an Transparenz hinsichtlich des Malware-Verhaltens und ist gleichzeitig vom Angreifer am schwersten zu erkennen.

Abbildung 3: Vollständige Systememulation als wirksamstes Mittel im Kampf gegen Malware

WatchGuard APT Blocker

Der neue Sicherheitsservice “APT Blocker” – der für alle UTM-Appliances von WatchGuard verfügbar ist – setzt auf vollständige Systememulation (CPU und Speicher), um detaillierte Einblicke in die Arbeitsweise von Malware-Programmen zu erhalten. Nachdem APT Blocker zunächst weitere Sicherheitsservices der UTM-Plattform abgefragt hat, werden die Fingerabdrücke der einzelnen Dateien mit einer bestehenden Datenbank abgeglichen – erst auf der Appliance selbst, anschließend in der Cloud. Wird die Datei nicht erkannt, erfolgt die Analyse mithilfe des Systememulators, der die Ausführung aller Befehle überwacht. Dieser identifiziert auch Ausweichtaktiken, die andere Sandbox-Systeme nicht erkennen.[5] Geprüft werden unterschiedlichste Dateitypen (siehe Kasten).

Von APT Blocker analysierte Dateitypen:

- **alle ausführbaren Windows-Dateien**
- **Adobe PDF**
- **Microsoft Office**
- **Android Application Installer Dateien (.apk)**
- **gepackte Dateien (.zip)**

Bei der Entwicklung des neuen Services APT Blocker erhielt WatchGuard Unterstützung von einem erfahrenen Partner. Lastline Technology wurde vom Techniker-Team gegründet, das auch Anubis entwickelt hat – das Werkzeug, das in den letzten acht Jahren auf der ganzen Welt eingesetzt wurde, um Dateien auf potenzielle Malware zu untersuchen.[6]

Sobald Malware erkannt wird, kann diese an der Firewall geblockt werden. In einigen Fällen lässt sich jedoch nicht ausschließen, dass ein Zero-Day-Schädling – der dem Namen wortwörtlich gerecht wird – durchschlüpft, während die Analyse in der Cloud noch läuft. In diesem Fall sendet das WatchGuard-System innerhalb weniger Minuten die Warnung, dass sich ein verdächtiger Code im Netzwerk eingeschlichen hat. Auf diese Weise können Administratoren umgehend nachforschen und Gegenmaßnahmen ergreifen.

Transparenz

Es reicht heutzutage nicht mehr aus, Malware bloß zu erkennen. Zudem benötigen IT-Verantwortliche klare, verwertbare Informationen, die nicht in einer Flut von Log-Daten untergehen. Denn die Herausforderung der IT-Abteilungen besteht darin, das Geschäft am Laufen zu halten, damit nicht zuletzt die gesetzten Umsatzziele erreicht werden. Trotz der weitreichenden Folgen, die eine Sicherheitsverletzung für ein Unternehmen haben kann, stehen zahlreiche IT-Abteilungen einschlägigen Security-Warnungen immer noch skeptisch gegenüber. So verzeichnete Neiman Marcus – ein weiteres US-amerikanisches Handelsunternehmen, das kürzlich gehackt wurde – über 60.000 Protokoll-Einträge, die darauf hindeuteten, dass Malware in das Netzwerk eingedrungen war.[7] Auch bei Target fand man wenige Tage nach dem ersten Übergriff etliche Log-Dateien, die auf ein Problem hinwiesen. Diese wurden jedoch ignoriert.[8]

[5] http://info.lastline.com/blog/next-generation-sandbox-offers-comprehensive-detection-of-advanced-malware

[6] http://info.lastline.com/blog/different-sandboxing-techniques-to-detect-advanced-malware

[7] http://www.businessweek.com/articles/2014-02-21/neiman-marcus-hackers-set-off-60-000-alerts-while-bagging-credit-card-data

[8] http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data#p1

Moderne Malware-Lösungen sollten sich durch folgende Merkmale auszeichnen:

- **Warnungen per E-Mail,** sobald eine schädliche Datei erkannt wird
- **Dokumentations- und Berichtsfunktionen,** die eng mit anderen Sicherheitsdiensten im Netzwerk verknüpft sind
- **klare Diagnosen und Informationen,** warum eine Datei als Malware eingestuft wurde, um eventuell vorschnelle Reaktionen zu vermeiden

WatchGuard APT Blocker erfüllt alle Visualisierungsanforderungen und bietet neben E-Mail-Benachrichtigungen oder Log-Analysen in Echtzeit auch die Möglichkeit, die relevanten Informationen bei Bedarf tiefer zu durchdringen. Der neue Service ist vollständig in die preisgekrönte Visualisierungslösung WatchGuard Dimension™ – die Kunden beim Einsatz einer UTM-Lösung von WatchGuard kostenlos nutzen können – integriert und beschränkt sich nicht allein auf den Hinweis, dass eine Datei verdächtig ist. Stattdessen erhält der Anwender zu jeder erkannten Malware-Datei einen detailierten Bericht, der das spezifische Verhalten und Auffälligkeiten im Einzelnen auflistet.

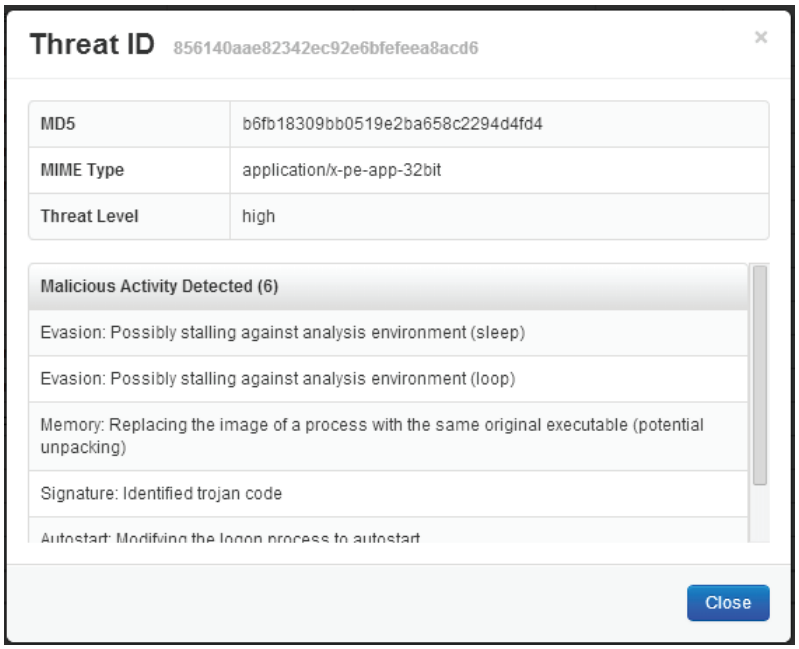

Abbildung 4: Ein APT-Bericht führt das Malware-Verhalten im Detail auf und erklärt, warum eine Datei als Malware markiert wurde.

Die Datei im oben gezeigten Beispiel weist gleich mehrere Malware-typische Merkmale auf. Die beiden gelisteten Ausweichmanöver (Evasion) verdeutlichen, wie APT Blocker arbeitet. Das System ist in der Lage, schädliche Aktivitäten aufzudecken, die andere Sandbox-Lösungen überfordert hätten.

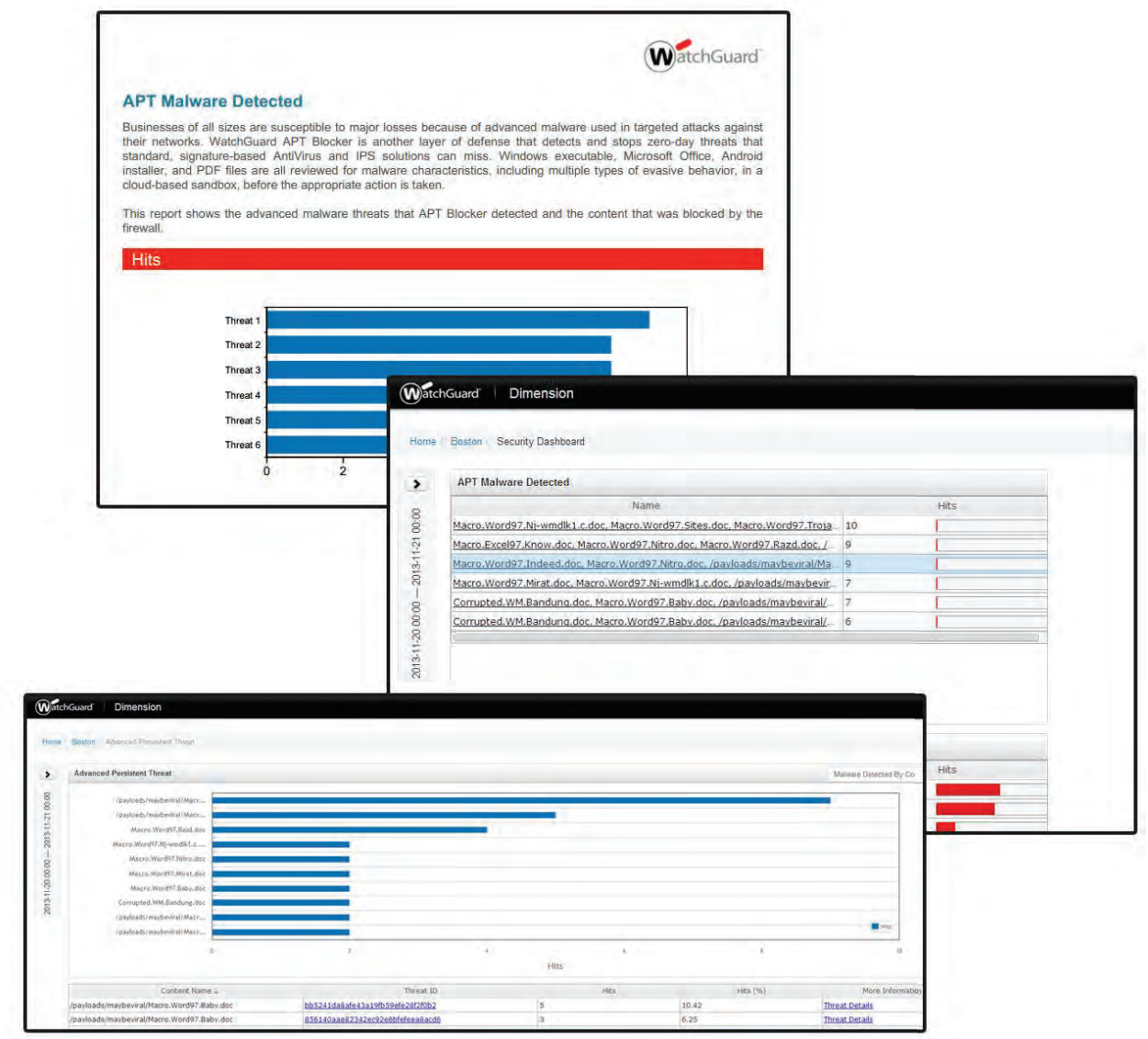

Abbildung 5: Im Security Dashboard von WatchGuard Dimension laufen die Informationen von APT Blocker und weiteren UTM-Services gezielt zusammen.

WatchGuard Dimension veranschaulicht die sicherheitsrelevanten Aktivitäten, die von einzelnen Diensten wie APT Blocker erfasst werden, par excellence und ermöglicht Administratoren bei Bedarf den sofortigen Zugriff auf weitere, ausführlichere Informationen. Zudem bietet das Tool mehr als 70 umfassende Berichtsvorlagen, wobei sich die Zustellung der Berichte an einzelne Empfänger innerhalb des Unternehmens per E-Mail gezielt festgelegen lässt. Die Auswahl umfasst neben Zusammenfassungen und Detailansichten ebenso spezifische Reports hinsichtlich HIPAA- oder PCI-Vorgaben. Darüber hinaus gibt es prägnante Executive Reportings für die Geschäftsleitung, IT-Leiter, Compliance-Beauftragte und Geschäftsführer kleinerer Unternehmen.

Maximaler Datenschutz dank moderner Malware-Identifizierung

Bedrohungen sind heute ausgefeilter als früher. Hacker nutzen heutzutage immer öfter Methoden, die in den letzten Jahren vorrangig bei IT-Angriffen auf staatliche Institutionen zum Einsatz kamen.

Lösungen zur Gefahrenabwehr müssen sich daher in gleichem Maße weiterentwickeln, um Unternehmen beim Schutz der Daten und Netzwerke die entscheidende Nasenlänge Vorsprung zu sichern. Das Aufspüren von Malware auf Basis von Signaturen reicht bei Weitem nicht mehr aus. Antiviren-Programme und Intrusion Prevention Systeme sind nach wie vor wichtige Elemente im Rahmen der IT-Sicherheit von Unternehmen. Nichtsdestotrotz sollten diese um moderne Analysemöglichkeiten ergänzt werden. Hierbei gilt es auf vier Schlüsselmerkmale zu achten:

1. **cloudbasierte Sandbox-Lösung mit vollständiger Systememulation** – mit der Möglichkeit, vielfältigste Dateitypen zu analysieren
2. **über die Sandbox hinausgehende Analyseoptionen,** um die verschiedenen Ausweichtaktiken von Malware zu identifizieren
3. **transparente Informationsdarstellung,** inklusive Warnfunktionen und Hinweisen, warum die entdeckte Malware entsprechend klassifiziert wurde
4. **über die reine Identifikation hinausgehende Handlungsmöglichkeiten**, um proaktiv reagieren und schädliche Dateien blockieren zu können

WatchGuard APT Blocker bietet dank cloudbasierter Sandbox mit vollständiger Systememulation umfassende Möglichkeiten, um moderne Malware und Zero-Day-Angriffe zu identifizieren und entsprechend abzuwehren.

Weitere Informationen zu WatchGuard APT Blocker unter www.watchguard.com/apt.

ADDRESSE:
Wendenstrasse 379
20537 Hamburg
Deutschland

WEB:
www.watchguard.de

DACH:
+49 (700) 9222 9333

Weltweit:
+1.206.613.0895

ÜBER WATCHGUARD
Seit 1996 entwickelt WatchGuard ganzheitliche Netzwerk- und Content-Sicherheitslösungen Unternehmen ihre Daten und Geschäfte umfassend schützen können. Das XTM-Portfolio (Ex Threat Management) kombiniert Firewall, VPN und Sicherheitsdienste. Die XCS-Appliances (I Content Security) schützen darüber hinaus Unternehmensinhalte sowohl in E-Mails als auch verhindern den Datenverlust. Dank umfangreicher Skalierungsmöglichkeiten hat WatchGuar Unternehmen jeder Größenordnung die passende Lösung und mehr als 15.000 eigens ausge Partner in 120 Ländern bieten abgestimmten Service. Der Hauptsitz von WatchGuard liegt in US-Bundesstaat Washington. Weitere Informationen unter www.watchguard.com.