LÖSUNGEN VON KASPERSKY LAB AUTOMATIC EXPLOIT PREVENTION TECHNOLOGY

The Power of Intelligence

www.kaspersky.de

1. DIE NEUE BEDROHUNG KOMMT VON INNEN

Im Jahr 2012 kamen beachtliche 87 % der Schwachstellen in Programmen von Drittanbietern vor[1]. Im selben Jahr registrierte Kaspersky Lab mehr als 132 Millionen risikobehaftete Programme.

„Wir bei Kaspersky Lab glauben, dass die effektivste Antwort auf diese sich rasch ausbreitende Bedrohung in einer Technologie besteht, die spezifischen Schutz vor Exploits bietet, die auf Schwachstellen in beliebten Programmen abzielen."

Fehler in Oracle Java, Adobe Flash Player und Adobe Reader sowie Schwachstellen in Microsoft Office sind die beliebtesten Angriffsziele für Kriminelle. Im Zeitraum März bis August 2013 registrierten die Experten bei Kaspersky Lab 8,54 Millionen Angriffe mithilfe von Java-Exploits: eine Zunahme von 52,7 % gegenüber dem vorhergehenden Halbjahreszeitraum.

Wir bei Kaspersky Lab glauben, dass die effektivste Antwort auf diese sich rasch ausbreitende Bedrohung in einer Technologie besteht, die spezifischen Schutz vor Exploits bietet, die auf Schwachstellen in beliebten Programmen abzielen. Indem verhindert wird, dass dieser schädliche Code überhaupt ausgeführt werden kann, werden wichtige Programme und Komponenten innerhalb der Unternehmensinfrastruktur nicht zu Einfallstoren für groß angelegte Angriffe.

1 Secunia Vulnerability Review 2013, Secunia Research Lab, 14. März 2013

2. SCHWACHSTELLEN ALS EINFALLSTORE – TYPISCHE EXPLOIT-METHODEN

Der Zweck von Exploits besteht in der Ausnutzung von Schwachstellen in weit verbreiteter Software mit dem Ziel, unterschiedliche Arten von Schadcodes auszuführen. Um ein System auf diese Art zu infizieren, bedienen sich Kriminelle einer großen Bandbreite unterschiedlicher Verfahren, u. a.:

- Benutzer werden auf eine speziell dafür vorgesehene schädliche Website bzw. eine mit einem Schadcode infizierte Website gelockt. Bei sogenannten „Watering-Hole-Attacken" haben es die Kriminellen auf Websites abgesehen, die bei bestimmten Benutzertypen, z. B. Entwicklern in Großunternehmen, besonders beliebt sind.
- Benutzer werden dazu verleitet, ein eigens angelegtes, echt oder harmlos aussehendes PDF- oder Office-Dokument oder ein Bild herunterzuladen oder zu öffnen.
- Mit Malware infizierte Wechseldatenträger, z. B. USB-Laufwerke, lassen sich problemlos in ein Unternehmen einschmuggeln. Bei Studien aus den letzten Jahren kam heraus, dass Mitarbeiter die auf dem Firmenparkplatz gefundenen USB-Sticks fast ausnahmslos an ihren Computer anschlossen, besonders dann, wenn die Sticks als Firmeneigentum gekennzeichnet waren.[2]

In der Regel beginnen gezielte Angriffe mit einem speziell gestalteten, schädlichen E-Mail-Anhang, der auf den ersten Blick echt aussieht und deshalb vom Benutzer geöffnet wird.

2 Bruce Schneier, „Yet Another 'People Plug in Strange USB Sticks' Story" (Noch ein Bericht über Menschen, die fremde USB-Sticks benutzen), Schneier on Security, https://www.schneier.com/blog/archives/2011/06/yet_another_peo.html

Weitere Informationen über Exploits, die über Wechseldatenträger eingeschleust werden, finden Sie unter: http://www.securelist.com/en/blog/208187475/Another_usb_media_infection

3. BELIEBTHEIT MACHT ANFÄLLIG – DIE AM HÄUFIGSTEN ATTACKIERTEN SOFTWARE-ARTEN

Fast jede Software weist Programmierfehler auf, wobei einige von ihnen die unbefugte Ausführung von schädlichem Code ermöglichen. Bei durchschnittlich 72 Programmen, die ein Benutzer auf seinem Computer installiert hat[3], ergeben sich folglich für ein Unternehmen eine Menge potentieller Schwachstellen. In Wirklichkeit konzentrieren sich Cyberkriminelle jedoch meist auf die populärsten Programme, da so eine möglichst große Anzahl potentieller Opfer garantiert ist. Denn ein Benutzer, der auf einen Malware-Link klickt, genügt ja schon …

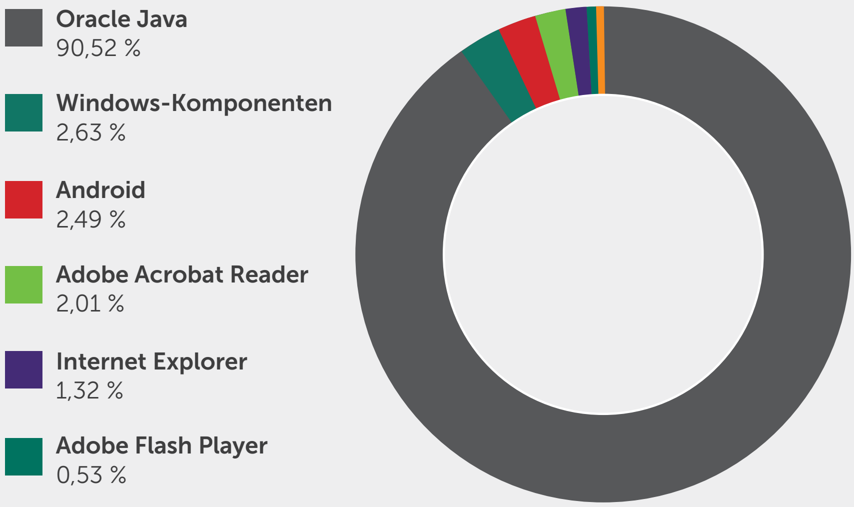
„Von unseren Kunden, die ihre Daten für unser Cloud-basiertes Kaspersky Security Network zur Erkennung und Analyse von Bedrohungen zur Verfügung stellen, arbeiten 6,3 % immer noch mit Windows XP."

Aus Untersuchungen bei Kaspersky Lab für das Jahr 2013 geht hervor, dass Oracle Java mit 90,52 % aller erkannten Exploit-Versuche die am meisten von Exploits angegriffene Software war. Die Schwachstellen werden durch Drive-by-Attacken im Internet ausgenutzt, und mittlerweile gibt es eine Vielzahl so genannte „Exploit-Packs" mit neuartigen Java-Exploits.[4]

Das zweitbeliebteste Ziel für Exploits stellen die Windows-Komponenten dar, z. B. anfällige Windows-Systemdateien, mit Ausnahme von Internet Explorer und Microsoft Office, für die Kaspersky Lab eine getrennte Kategorie vorgesehen hat. Die meisten Angriffe in dieser Kategorie haben es auf eine Schwachstelle abgesehen, die in win 32k.sys-CVE-2011-3402 entdeckt und zuerst für den berüchtigten Duqu-Exploit eingesetzt wurde.

3 Secunia Vulnerability Review 2013.

4. Kaspersky Lab Report: Java Under Attack – The Evolution of Exploits in 2012-2013, Securelist, 30. Oktober 2013, http://www.securelist.com/en/analysis/204792310/Kaspersky_Lab_Report_Java_under_attack_the_evolution_of_exploits_in_2012_2013



Schwachstellen in Oracle Java machen die überwältigende Mehrheit von Exploits aus[5]

Mit der Zeit ändert sich die Rangfolge der am häufigsten angegriffenen Software-Arten. So war Microsoft Office im Jahr 2010 das beliebteste Angriffsziel. Da Microsoft Windows XP und Office 2003 im April 2014 auslaufen ließ, werden keine Sicherheitsupdates und Patches mehr für diese Software zur Verfügung gestellt. Hierdurch werden einige Unternehmen anfällig für Schwachstellen, auf die Cyberkriminelle höchstwahrscheinlich bereits ein Auge geworfen haben. Von unseren Kunden, die ihre Daten für unser Cloud-basiertes Kaspersky Security Network zur Erkennung und Analyse von Bedrohungen zur Verfügung stellen, arbeiten 6,3 % immer noch mit Windows XP.

5 http://www.securelist.com/en/images/vlill/stat_ksb_2013_04.png

4. ALLGEMEINE SCHUTZMETHODEN VOR EXPLOITS

Die Lösungen von Kaspersky Lab bedienen sich unterschiedlicher Methoden, um Exploits zu blockieren. Es werden beispielsweise spezielle Signaturen für Malware hinzugefügt, die auf Exploits basieren, damit schädliche Dateien (z. B. E-Mail-Anhänge) erkannt werden können, noch bevor sie geöffnet werden. Proaktiver Schutz und andere Technologien erlauben die Erkennung und Blockierung von Malware, nachdem eine infizierte Datei geöffnet wurde. Schließlich ermöglicht das Vulnerability Scanning die problemlose Erkennung von anfälliger Software auf beliebigen Endpoints und kann im Zusammenspiel mit dem Patch Management sowie anderen Systems-Management-Funktionen automatisch Updates anwenden und so verhindern, dass ungepatchte Software gestartet wird.

„Selbst wenn nur vergleichsweise wenige Bedrohungen den herkömmlichen Schutzmechanismen entgehen, so macht der massive Schaden, der von nur einem nicht erkannten Exploit angerichtet werden könnte, eine zusätzliche Schutzschicht für das Unternehmen zwingend erforderlich."

Natürlich lassen sich die meisten Exploits verhindern, wenn die Windows-Systemkomponenten und andere installierte Software regelmäßig aktualisiert werden.

In einigen Fällen helfen die üblichen Schutzmethoden jedoch nicht weiter. Dies gilt insbesondere für die so genannten Zero-Day-Schwachstellen, d. h. noch gar nicht oder erst vor kurzem entdeckte Fehler in einer Software. In diesem Fall ist es für Anbieter von Sicherheitssoftware sehr schwierig, Exploits, die es auf diese Schwachstellen abgesehen haben, mithilfe signaturbasierter Methoden zu erkennen. Aufwändige Exploits bedienen sich darüber hinaus oft einer Vielzahl von Methoden, um proaktive Schutztechnologien zu umgehen bzw. zu überwinden. Selbst wenn nur vergleichsweise wenige Bedrohungen den herkömmlichen Schutzmechanismen entgehen, so macht der massive Schaden, der von nur einem nicht erkannten Exploit angerichtet werden könnte, eine zusätzliche Schutzschicht für das Unternehmen zwingend erforderlich. Genau hier kommt der automatische Exploit-Schutz ins Spiel.

5. AUTOMATISCHER EXPLOIT-SCHUTZ: FUNKTIONSWEISE

Der automatische Exploit-Schutz richtet sich speziell gegen Malware, die Schwachstellen in Software ausnutzt, um Endpoints und Netzwerke von Unternehmen zu infizieren. Selbst wenn ein Benutzer eine schädliche Datei bereits heruntergeladen und geöffnet hat, verhindert die AEP-Technologie das Ausführen der Malware.

Die Entwicklung von AEP bei Kaspersky Lab basiert auf einer tiefgreifenden Analyse des Verhaltens und der Charakteristika von weit verbreiteten Exploits. Hierdurch ist unsere Technologie in der Lage, die für Exploits charakteristischen Verhaltensmuster zu erkennen und zu blockieren.

Während der Entwicklung erhielten unsere Forschungs- und Entwicklungsteams tiefgreifende Einblicke in die am häufigsten attackierten Geschäftsprogramme und passten die AEP-Technologie entsprechend an. AEP ist jetzt Teil unserer Antiviren- und Internet-Sicherheitslösungen, wo es zusammen mit unserem Aktivitätsmonitor eine zusätzliche Schutzschicht bereitstellt, welche die folgenden Funktionen bietet:

KONTROLLE ÜBER POTENTIELL ANFÄLLIGE PROGRAMME

Bei der AEP-Technologie wird den am häufigsten attackierten Programmen, wie Adobe Reader, Internet Explorer und Microsoft Office, besondere Bedeutung eingeräumt. Jeder Versuch dieser Programme, ungewöhnliche Programmdateien oder Code auszuführen, löst zusätzliche Sicherheitskontrollen aus. In vielen Fällen sind diese Aktivitäten berechtigt, z. B. wenn Adobe Reader eine Programmdatei startet, um nach Updates zu suchen. Es gibt jedoch bestimmte Charakteristika von Programmdateien, die zusammen mit verknüpften Aktionen auf schädliche Aktivitäten hinweisen und deshalb eine zusätzliche Überprüfung erfordern.

ÜBERWACHUNG VON VORGÄNGEN VOR DEM PROGRAMMSTART

Die Art und Weise, wie ein Programm gestartet oder Code ausgeführt wird, und was kurz davor genau passiert, ist sehr aussagekräftig. Bestimmte Verhaltensmuster weisen stark auf eine schädliche Aktivität hin; unsere AEP-Technologie ist in der Lage, diese Aktivität zu ihrem Ursprung zurückzuverfolgen. Dieser könnte in der Software selbst liegen, aber auch das Resultat eines Exploits sein. Statistische Daten zu charakteristischem Exploit-Verhalten tragen dazu bei, diese Art von Aktivitäten zu identifizieren, selbst dann, wenn eine Zero-Day-Schwachstelle ausgenutzt wird. Mit anderen Worten: Zum Erkennen einer schädlichen Aktivität ist es für AEP nicht erforderlich, die Schwachstelle, die ausgenutzt werden soll, genau zu kennen.

CODE ZUM URSPRUNG ZURÜCKVERFOLGEN

Bestimmte Arten von Exploits, insbesondere jene, die bei Drive-by-Angriffen (d. h. Exploits, die über schädliche Webseiten verbreitet werden) eingesetzt werden, müssen ihre „Nutzlast“ erst von einer anderen Webseite abholen, bevor sie sie ausführen. Die AEP kann solche Dateien zu ihrem Ursprung zurückverfolgen, exakt bestimmen, welcher Browser den Download ausgeführt hat, und die Remote-Webadresse der Dateien abrufen.

„Durch Kasperskys Methode des auf Überprüfung und Überwachung basierenden Ansatzes sowie der tiefgreifenden Analyse und der kontinuierlichen Forschung, die wir für beliebte Unternehmensprogramme betreiben, ist das Risiko von Fehlalarmen äußerst gering.“ Sie können dieses Feature auch im interaktiven Modus ausführen. “

Außerdem ist die AEP bei machen Programmen in der Lage, zwischen Dateien zu unterscheiden, die mit Einverständnis des Benutzers erstellt wurden, und solchen, die ohne Einwilligung hinzugefügt wurden. Wird der Versuch unternommen, einen verdächtigen Code auszuführen, kann diese Information dazu beitragen, einen Exploit zu identifizieren und zu blockieren.

EXPLOITS AN DER AUSNUTZUNG DER SCHWACHSTELLE HINDERN

Die AEP setzt bei einigen Programmen und Softwaremodulen das so genannte Address Space Layout Randomization-Verfahren (ASLR, deutsch etwa Zufallsgestaltung des Adressraum-Aufbaus) ein, um zu verhindern, dass Exploits die spezielle Schwachstelle bzw. den Code finden, der ausgeführt werden soll.

Das ASLR-Verfahren ist seit Vista Bestandteil der Microsoft Windows-Betriebssysteme, aber nicht alle Programme unterstützen diese Standardfunktion. Die AEP-Technologie von Kaspersky Lab stellt die ASLR-Funktionalität auch für Programme zur Verfügung, welche diese Standardversion nicht unterstützen. So kann verhindert werden, dass bestimmte Arten von Exploits die Position des Codes, der ausgeführt werden soll, im Arbeitsspeicher ausfindig machen können. Wiederholte Versuche, den gewünschten Code ausfindig zu machen, führen eher zu einem Programmabsturz als zur Ausführung des schädlichen Codes.

In welchen Lösungen ist AEP integriert?

Die AEP-Technologie ist in Kaspersky Endpoint Security for Business integriert. Sie ist standardmäßig aktiviert, kann aber einzeln oder zusammen mit dem Aktivitätsmonitor-Modul (welches die Programmaktivität im gesamten System überwacht) deaktiviert werden.

Standardmäßig blockiert die AEP die Ausführung von verdächtigem Code. Dank unseres auf Überprüfung und Überwachung basierenden Ansatzes sowie der tiefgreifenden Analyse und der kontinuierlichen Forschung, die wir für beliebte Unternehmensprogramme betreiben, ist das Risiko von Fehlalarmen äußerst gering. Sie können dieses Feature auch im interaktiven Modus ausführen.

6. DIE VORTEILE FÜR IT-SICHERHEIT IN UNTERNEHMEN

Der automatische Exploit-Schutz reduziert erheblich das Risiko von Infektionen durch weit verbreitete Malware oder gezielte Exploit-Attacken, inkl. Zero-Day-Exploits. Während ausgedehnter interner Test-, Forschungs- und Entwicklungsreihen konnten mithilfe von AEP Exploits für weit verbreitete Schwachstellen in Adobe Flash Player, QuickTime Player, Adobe Reader, Java und anderen Programmen erfolgreich blockiert werden.

Der IT-Sicherheitsansatz von Kaspersky Lab hat schon immer auf einer mehrschichtigen Verteidigung basiert, die durch eine effektive Analyse des Bedrohungspanoramas ergänzt wird, um den Charakter bis dato unbekannter Bedrohungen vorherzusehen. Der automatische Exploit-Schutz blockiert die Ausführung von bekannten und unbekannten Exploits. Hierdurch werden andere Kaspersky-Technologien, z. B. der Viren- und Spam-Schutz, um ein Sicherheitsnetz ergänzt, das komplexen Code abfangen kann, der traditionelle IT-Sicherheitstechnologien umgeht.

Kaspersky Lab hat sich langfristig der Antizipation und Verhinderung von IT-Sicherheitsrisiken verschrieben, um das Risiko für Unternehmen heute und in einer immer komplexer werdenden Zukunft zu reduzieren.

Twitter.com/
Kaspersky_DACH

Facebook.com/
Kaspersky.Lab.DACH

Youtube.com/
KasperskyLabCE

Kaspersky Labs GmbH,
Ingolstadt, Deutschland
www.kaspersky.de

Informationen zur
Internetsicherheit:
www.viruslist.de

Informationen zu Partnern in
Ihrer Nähe finden Sie hier:
http://www.kaspersky.com/de/
partner_finden