SOPHOS
Security made simple.

# Exploits in der Falle

Exploits sind eine der beliebtesten Methoden zur Verbreitung von Malware. Sie nutzen Schwachstellen in legitimen Software-Produkten wie Flash und Microsoft Office aus, um Computer für kriminelle Zwecke zu infizieren. Ein einziger Exploit kann von verschiedensten Malware-Varianten mit jeweils unterschiedlichen Payloads genutzt werden.

Antivirus-Lösungen haben sich bislang darauf konzentriert, Malware zu stoppen, die Exploits nutzt, anstatt die Exploits selbst zu bekämpfen. Ein fataler Irrtum. Denn obwohl Millionen verschiedener Malware-Varianten im Umlauf sind, nutzen Hacker nur etwa 10 verschiedene Verfahren, um Software-Schwachstellen auszunutzen. Wenn es also gelingt, diese Exploit-Verfahren zu unterbinden, kann auf einen Schlag eine beträchlichte Anzahl von Malware-Samples blockiert werden, bevor sie auf Systemen Fuß fassen kann. So lassen sich sogar Exploits in Form von Drive-By-Angriffen und Zero-Day-Schwachstellen blockieren.

In diesem Whitepaper erfahren Sie mehr über Exploits und effektive Abwehrmaßnahmen. Wir erklären, wie Exploits und die Exploit-Branche funktionieren, was in den Augen von Cyberkriminellen einen guten Exploit ausmacht und wie Sie Ihr Unternehmen mit Anti-Exploit-Technologien wirksam und effizient vor komplexen und unbekannten Bedrohungen schützen können.

Sophos-Whitepaper September 2016

# Exploits und Exploit-Kits

## Exploits

Bei den meisten Cyberangriffen nutzen Kriminelle Sicherheitsschwachstellen aus. Beispiele für solche Schwachstellen sind: ein unsicheres Passwort, ein Benutzer, der auf einen gefälschten Anmeldelink hereinfällt, ein Dateianhang, den jemand unachtsam öffnet, oder lediglich der Besuch einer infizierten Übertragungsseite, ohne dass Elemente auf der Seite angeklickt werden. Die Angriffe sind sehr hinterlistig und können selbst besonders achtsame Benutzer hinters Licht führen. Unter der Bezeichnung **Exploit** verstehen wir die Ausnutzung eines Software-Bugs, um eine oder mehrere vorhandene Sicherheitsbarrieren zu umgehen.

Software-Bugs, die sich auf diese Weise ausnutzen lassen, werden als **Schwachstellen** bezeichnet und können viele Formen annehmen. Ein Homerouter kann beispielsweise eine Passwortseite mit einem heimlichen „Backdoor-Code" besitzen, über den sich ein Betrüger selbst dann anmelden kann, wenn Sie ein individuelles Passwort eingerichtet haben. Oder ein von Ihnen genutztes Software-Produkt hat einen Bug, der bei unerwarteten Eingaben (z. B. überlanger Benutzername oder Bild mit ungewöhnlicher Größe) zum Systemabsturz führt.

Viele Software-Bugs verursachen Fehler, die lästig sind, vom Betriebssystem jedoch erkannt und sicher gehandhabt werden können. Eine Schwachstelle hingegen ist ein Bug, der orchestriert bzw. kontrolliert werden kann, sodass er nicht autorisierte und unsichere Aktionen ausführt (z. B. Programmabstürze, bevor das Betriebssystem eingreifen und Sie schützen kann).

Angreifer nutzen solche Schwachstellen meist, indem sie eine der von Ihnen genutzten Anwendungen – wie Ihren Browser oder das Textverarbeitungsprogramm – zur Ausführung eines kleinen Programms oder Programmfregments manipulieren, das von außen ins Netzwerk gelangt ist. Durch den Einsatz eines sogenannten Remote Code Execution Exploit (oder kurz RCE) kann ein Angreifer jegliche Sicherheits-Pop-ups und Warndialoge unterdrücken, sodass Sie keine Chance haben, den Angriff zu stoppen.

Von Zero-Day-Exploits sprechen wir, wenn Hacker eine noch weitgehend unbekannte Schwachstelle ausnutzen, für die noch kein Patch verfügbar ist.

Da Exploits Schwachstellen in legitimer Software ausnutzen, die oft noch unbekannt sind, ist es schwer, sich zu schützen – selbst wenn Security Best Practices befolgt werden.

## Exploit-Kits

**Exploit-Kits** sind vorverpackte Toolkits mit Schadwebseiten oder -software, die Kriminelle kaufen, lizenzieren oder leasen können, um Malware in Umlauf zu bringen. Mit anderen Worten: Wenn Sie eine neue Malware – vielleicht Ransomware, einen Trojaner oder einen Password Stealer – haben, können Sie diese Malware mit einem Exploit-Kit an nichtsahnende Opfer übertragen.

Anstatt selbst herauszufinden, wie Sie Ihre eigenen Webseiten so präparieren können, dass Besucher infiziert werden, verlassen Sie sich auf einen vorgefertigten Angriffscode in einem Exploit-Kit, der eine Reihe bekannter Sicherheitslücken in der Hoffnung austestet, dass eine funktioniert.

Ein Exploit-Kit wird normalerweise in Form eines verschachtelten und schwer nachzuverfolgenden JavaScripts direkt in den Browser des potenziellen Opfers eingeschleust und testet dort automatisch eine Serie von Angriffen (meist in der wahrscheinlichsten Abfolge), bis einer der Angriffe funktioniert. Falls keiner funktioniert, sieht das in etwa so aus:

```
if java installed then
   try java exploit 1
   if exploit worked then install malware end
end
if silverlight installed then
   try silverlight exploit 1
   if exploit worked then install malware end
   try silverlight exploit 2
   if exploit worked then install malware end
end
if flash is installed then
   ...
end
if nothing worked then give up end
```

Dasselbe Exploit-Kit kann zur Übertragung mehrerer verschiedener Malware-Samples verwendet werden; und dasselbe Malware-Sample kann von einem oder mehrenden verschiedenen Exploit-Kits übertragen werden.

```
<script>var wqncvnhankfhte=(1194000100<780281714?"ie":"rv:1");
var gjxtcjftwwxi=(1149318224+131959385<1122077856+259936926?"gjx":"dk");
var fntzefklgaqvsjy=(1577258313>1944482977?"w":"r");
var wmjsvibonuq=(1293847248>1687638986?"rtr":"\x72\x65\x74\x75\x72\x6e");
wqnctvnankfhte+=(151554506+472333707>363202458?"\x31":"\x68\x74");
var ixgjdotdmfrbi=(160750077+525999200>1876280?"\x5b\x5d":"\x74");
var gfanlterj=(2103263286>2143916270?"czr":"ret");
var wqkbimsjzmmaf=(968162729<189979742?"\x6b":"wq");
var rggshjhsixeofuo=(115809819+1034707353<1078015506+1085801417?"\x72":"c");
fntzefklgasjy+=(77641620+817194218<1256743977+344513278?"\x65\x74":"\x71\x6f");
```

Convoluted JavaScript code from an Angler exploit kit web page

Neben Exploit-Kits, die als Übertragungsweg das Internet nutzen, existieren auch eine Reihe ähnlicher Exploit-Kits für E-Mail- und Phishing-Kampagnen. Bei diesen versendet der Angreifer einen Dateianhang an nichtsahnende Nutzer in der Hoffnung, dass diese den Anhang öffnen, das Exploit-Kit installieren oder sich die Bilder in der E-Mail anzeigen lassen. Es existiert eine Vielzahl von Bereitstellungsmechanismen und die ahnungslosen Opfer haben wenig Chance gegen diese raffinierten Angriffe, wenn sie ihre Computer und Smartphones weiterhin nutzen möchten.

## Die Exploit-Branche

Dank Exploit-Kits müssen sich Malware-Autoren keine Gedanken darüber machen, wie sie in Java, Silverlight oder Flash Bugs finden, wie sie aus diesen Bugs Exploits machen, wie sie unsichere Web-Server zum Hosten von Exploits finden, oder wie sie potenzielle Opfer auf schädliche Webseiten locken.

Gleichzeitig müssen die Exploit-Kit-Autoren selbst keine Malware schreiben. Sie müssen keine Server betreiben, um infizierte Computer im Auge zu behalten, oder Geld von einzelnen Opfern eintreiben. Sie müssen keine Daten abschöpfen, diese Daten nicht weiterverkaufen usw.

Jede Gruppe spezialisiert sich auf einen oder mehrere Teile der Bedrohungslandschaft – in einem System, das mittlerweile satirisch als Crimeware-as-a-Service oder kurz CaaS bezeichnet wird. Und zwischen ihnen stehen die Exploit-Broker.

Exploit-Broker kaufen Exploits von Personen, die diese entdecken, und verkaufen sie an Interessierte weiter. Dies können staatliche Stellen genauso sein wie ruchlose Hacker. Eines haben jedoch all diese Interessenten gemein: Sie behalten ihre Motive gerne für sich. Kevin Mitnick, der Gründer von Mitnick's Absolute Zero Day Exploit Exchange erklärt Wired:

*„Wenn einer unserer Kunden eine Zero-Day-Schwachstelle kaufen möchte, stellen wir keine Fragen und würden, selbst wenn wir das täten, keine Antwort erhalten.*

*Forscher finden die Schwachstellen, verkaufen sie für X an uns, wir verkaufen Sie für Y an unsere Kunden und streichen die Gewinnmarge durch den Weiterverkauf ein."*

https://www.wired.com/2014/09/kevin-mitnick-selling-zero-day-exploits/

Exploits zu verkaufen, ist nicht illegal, aber lukrativ. Jährliche Abonnements für 25 Zero-Day-Schwachstellen werden für bis zu 2,5 Mio. UDS gehandelt.

## Warum Patches so wichtig sind

Wie bereits erwähnt, nutzen Exploits Schwachstellen in legitimen Software-Produkten aus. Alle renommierten Software-Anbieter entwickeln daher nach der Meldung von Schwachstellen Patches zur deren Behebung. Am bekanntesten sind hier wohl die Patches von Microsoft, die an jedem zweiten Dienstag im Monat (Patch Tuesday) veröffentlicht werden. Zwischen dem Aufdecken einer Schwachstelle und der Entwicklung eines Patches besteht fast immer eine gewisse zeitliche Verzögerung – auch dann, wenn bekannt ist, dass die Schwachstelle für kriminelle Machenschaften ausgenutzt wird. So auch bei der Sicherheitslücke CVE-2016-4171, wie aus folgendem Adobe-Sicherheitshinweis vom 14. Juni 2016 hervorgeht:

*„Bei Adobe Flash Player 21.0.0.242 und früheren Versionen für Windows, Macintosh, Linux und Chrome OS besteht eine kritische Sicherheitslücke (CVE-2016-4171). Ein erfolgreicher Angriff kann zum Absturz der Applikation führen und einem Angreifer die Übernahme des betroffenen Systems ermöglichen.*

*Adobe wurde berichtet, dass ein Exploit für CVE-2016-4171 existiert und für begrenzte gezielte Angriffe verwendet wird. Adobe wird diese Sicherheitslücke durch das monatliche Sicherheitsupdate schließen, das bereits am 16. Juni verfügbar ist.“*

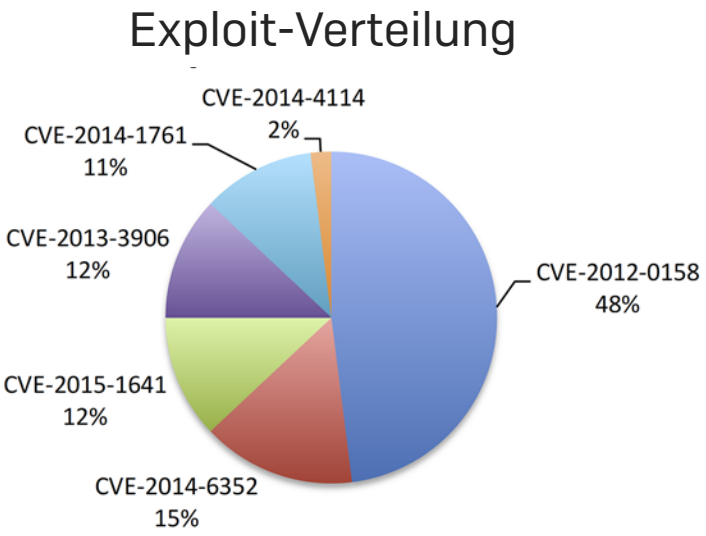
In der Regel sollten die Tage einer Schwachstelle nach Veröffentlichung eines Patches gezählt sein, da immer mehr Benutzer ihre Software aktualisieren und demzufolge immer weniger anfällig für die Schwachstelle sind. Dies hängt jedoch immer davon ab, wie schnell und effektiv Unternehmen Schwachstellen patchen. Wie CVE-2012-0158 zeigt, sind nachlässige Patching-Routinen für Cyberkriminelle ein gefundenes Fressen.

## Anatomie eines erfolgreichen Exploits: Die Schwachstelle CVE-2012-0158

CVE-2012-0158 ist eine der am häufigsten ausgenutzten Schwachstellen des letzten Jahrzehnts, deren Langlebigkeit nicht zuletzt auf ihre konstante Anpassungsfähigkeit zurückzuführen ist: Man könnte auch von einer modernen Version von Charles Darwins „Über die Entstehung der Arten“ sprechen.

Öffentliches Aufsehen hat CVE-2012-0158 mit einer Reihe gut dokumentierter, gezielter Angriffe wie Red October, FakeM und der Rotten Tomato Campaign erregt. Die explizit ausgewählten Opfer in diesen Fällen reichten von der Logistikbranche über Lederunternehmen bis hin zu Diplomaten-Vereinigungen und staatlichen Organisationen. CVE-2012-0158 scheint also nicht nur sehr beliebt zu sein, sondern wird auch von unterschiedlichen Gruppen Krimineller mit verschiedenen Motiven verwendet.

CVE-2012-0158 wurde von Microsoft (MS12-027) bereits im Jahr 2012 gemeldet und gepatcht, büßte jedoch auch danach in Hackerkreisen kaum an Beliebtheit ein. Tatsächlich führte CVE-2012-0158 selbst im letzten Quartal des Jahres 2015 die Exploit-Statistik der *SophosLabs* weiterhin an und war für ganze 48 % aller gemeldeten Word-basierten Exploit-Angriffe verantwortlich.




Exploit-Verteilung, Oktober – Dezember 2015
Quelle: SophosLabs

Dass Cyberkriminelle eine bestimmte Schwachstelle bevorzugen, ist grundsätzlich nichts Ungewöhnliches. Dass eine Schwachstelle aber über so viele Jahre erfolgreich bleibt, ist sehr außergewöhnlich. Wird eine Schwachstelle gepatcht, sind ihre Tage meist gezählt: Denn je mehr Personen den Patch installieren, desto unwirksamer wird die Schwachstelle. Wenn man bedenkt, dass für CVE-2012-0158 im April 2016 bereits seit vier Jahren ein Patch von Microsoft verfügbar war, ist es erstaunlich, dass Cyberkriminelle nach wie vor in der Lage sind, diesen Exploit auszunutzen.

## Was erwartet uns in Sachen CVE-2012-0158 als Nächstes?

Solange sich die Office-Exploit-Kits nicht von CVE-2012-0158 lossagen, wird CVE-2012-0158 wohl kaum in absehbarer Zeit von der Bildfläche verschwinden. Dass der Exploit weiterhin genutzt wird, spricht dafür, dass er nach wie vor erfolgreich ist; auch wenn er seine Strategie von Spam-Kampagnen auf konzentriertere Angriffe umstellen musste. Wenn es auf der Welt noch ungepatchte Computer gibt, ist davon auszugehen, dass Exploit-Kit-Autoren weiterhin an CVE-2012-0158 festhalten.

Die Existenz von CVE-2012-0158 ist also nicht bedroht, vielmehr jedoch seine Position am oberen Ende der Exploit-Charts. Im letzten Jahr sind neuere und lukrativere Schwachstellen aufgetaucht, die bereits in Exploit-Kits integriert wurden und in Malware-Gruppen favorisiert werden. Am wahrscheinlichsten vom Thron stoßen könnten CVE-2012-0158 die RTF-Schwachstelle CVE-2015-1641, die eine Ausnutzung der Verarbeitung eingebetteter Inhalte durch Office ermöglicht, und die Schwachstelle CVE-2015-2545, mit der sich der Code ausnutzen lässt, den Office nutzt, um PostScript-Dateien zu analysieren.

## Was eine „gute“ Schwachstelle ausmacht

Die anfängliche Beliebtheit von CVE-2012-0158 war verständlich, weil diese Schwachstelle viele Kriterien erfüllt, nach denen Malware-Autoren bei der Wahl eines Droppers für ihre Spam-Kampagnen Ausschau halten. Spam-Kampagnen werden normalerweise an eine große Anzahl zufällig ausgewählter Empfänger versendet. Die Auswahl der Angriffstechnik kann also nicht unter Berücksichtigung der beim Opfer installierten Software erfolgen. Die Cyberkriminellen müssen stattdessen nach dem Wahrscheinlichkeitsprinzip vorgehen und auf eine Angriffstechnik setzen, die in den häufigsten Setups funktioniert. Anhand der folgenden vier Fragen ermitteln Cyberkriminelle, wie lohnend eine Schwachstelle für sie sein könnte:

1. **Ist das Dateiformat als E-Mail-Anhang unverdächtig?**

   Die meisten Sicherheitslösungen in Unternehmen entscheiden anhand des Dateityps, ob ein E-Mail-Anhang von externen E-Mail-Adressen ins Netzwerk gelangen darf.

   Der Code, den CVE-2012-0158 ausnutzt, befindet sich in der Microsoft Windows Common Control Library. CVE-2012-0158 betrifft explizit die ListView- und TreeView-ActiveX-Steuerelemente. Beide dieser Steuerelemente können in Word-Dokumenten und Excel-Tabellenblättern ausgenutzt werden und sowohl Word und Excel sind unauffällige Formate.

2. **Wie groß ist die Wahrscheinlichkeit, dass der Computer mit dem Angriff kompatibel ist?**

   Im Hinblick auf das Dateiformat ist außerdem zu beachten, ob das Opfer die richtige Software installiert hat, damit der Angriff beim Öffnen der Datei erfolgreich ablaufen kann. Die Wahrscheinlichkeit, dass eine Infektion mit einem AutoCAD Dropper erfolgreich ist, ist beispielsweise weit geringer als bei einem PowerPoint-Präsentations-Dropper.

   Von der CVE-2012-0158-Schwachstelle betroffen sind Microsoft Office 2003, 2007 und 2010. Office 2010 war zum Zeitpunkt der Bekanntmachung der Schwachstelle die aktuelle Version. Obwohl Alternativen zu Microsoft Office in jüngster Zeit auf dem Vormarsch sind, ist MS Office nach wie vor der Marktführer und macht CVE-2012-0158 damit zum perfekten Kandidaten.

3. **Welche Funktionalität ermöglicht der Angriff?**

   Ein unauffälliges, flächendeckend unterstütztes Dateiformat ist gut und schön, aber selbst die beste Technik ist nutzlos, wenn der Angriff nicht in der Lage ist, den Cyberkriminellen die gewünschte Funktionalität zu liefern.

   CVE-2012-0158 wird als „Arbitrary Code Execution“-Schwachstelle eingestuft. Dieser Schwachstellentyp gilt als einer der gefährlichsten, da er Hackern bei Ausnutzung erlaubt, die Kontrolle über das Programm (in diesem Fall Microsoft Word/Excel) zu übernehmen und es zu zwingen, ihre Befehle auszuführen.

4. **Wie flexibel ist diese Angriffsmethode darin, sich vor der Antivirus-Software zu verbergen?**

   Der Erfolg einer Angriffsmethode hängt zum großen Teil davon ab, wie anpassungsfähig sie ist. Sobald die Antivirus-Branche eine Angriffsmethode erkannt hat, beginnt ein Katz- und Mausspiel, bei dem die Malware ihr Erscheinungsbild stetig ändert, um nicht erkannt zu werden.

   Leider gelang es den Malware-Autoren in kürzester Zeit, geschickte Verfahren zu entwickeln, mit der die Präsenz von CVE-2012-0158 verschleiert werden kann:

   - Standardpasswortverschlüsselung
   - Verwendung des Rich-Text-Dateiformats
   - Leerzeichen und Verschleierung eingebetteter Gruppen
   - Vermischen von Binärdaten

# Methoden zum Schutz vor Exploits

## Anti-Exploit-Technologie

Obwohl Millionen verschiedener Malware-Varianten im Umlauf sind, nutzen Hacker nur etwa 10 verschiedene Verfahren, um Software-Schwachstellen auszunutzen. Diese Exploit-Verfahren zu blockieren, ist daher eine hoch effiziente und effektive Methode, um eine beträchtliche Anzahl von Malware-Samples auf einen Schlag unschädlich zu machen.

***Sophos Intercept X*** ist eine Next-Gen-Endpoint-Lösung mit leistungsstarken Anti-Exploit-Funktionen. Sophos Intercept X erkennt und blockiert Exploit-Verfahren und stoppt auf diese Weise alle Malware-Schädlinge, die diese Verfahren nutzen. Ob die Malware bereits bekannt ist, spielt keine Rolle: Intercept X erkennt einfach die Exploit-Verfahren und verhindert, dass diese zum Einsatz kommen. Im Gegensatz zu anderen Anti-Malware-Technologien stoppt Sophos Intercept X die Bedrohungen, bevor sie auf Ihr System gelangen. Ihre Infrastruktur wird somit weit weniger beeinträchtigt.

## Sicherheits-Best-Practices

Um Ihre Exploit-Abwehr zu verstärken, empfehlen wir Ihnen Folgendes:

**Installieren Sie Sophos Intercept X.** Sophos Intercept X kann gemeinsam mit Sophos Central Endpoint Protection Advanced sowie mit Endpoint-Lösungen anderer Antivirus- und Next-Gen-Anbieter genutzt werden, um Ihren Schutz weiter zu erhöhen. Bei einer Bereitstellung mit Sophos Endpoint wird Sophos Intercept X in einen zentralen Agenten integriert, der über eine zentrale Verwaltungsplattform gesteuert wird.

**Installieren Sie Patches rechtzeitig und regelmäßig.** Wenn Sie die Schwachstellen, auf deren Ausnutzung ein Exploit-Kit programmiert ist, bereits beseitigt haben, kann das Exploit-Kit Ihnen nichts mehr anhaben.

**Halten Sie Ihre Sicherheitssoftware auf dem neuesten Stand.** Eine gute Antivirus-Software kann über Dokumente erfolgende Angriffe an vielen Punkten blockieren: Sie kann beispielsweise gefährliche E-Mail-Anhänge beseitigen, bevor Sie diese öffnen, schädliche Websites herausfiltern und sperren sowie Schaddateien blockieren, sodass Sie diese nicht öffnen können.

**Ziehen Sie den Einsatz eines einfachen Dokumentviewers in Betracht.** Der Word Viewer von Microsoft ist zum Beispiel meist weit weniger anfällig als Microsoft Word selbst. Außerdem unterstützt er keine Makros, die gerne von Ransomware zweckentfremdet werden.

**Entfernen Sie ungenutzte Browser-Plug-ins.** Wenn Sie Java (bzw. Silverlight oder Flash) nicht in Ihrem Browser benötigen, deinstallieren Sie das Plug-in. Ein Exploit-Kit kann keine Browser-Komponente angreifen, die nicht vorhanden ist.

## Fazit

Exploits sind unglaublich leistungsstarke Tools, die von Cyberkriminellen heutzutage flächendeckend genutzt werden. Ein einziger Exploit kann dabei Millionen von Malware-Varianten in Umlauf bringen. Die gute Nachricht lautet: Wenn es Ihnen gelingt, diese Exploits aufzuhalten, können Sie den Großteil der Malware bereits stoppen, bevor sie auf Ihr System gelangt.

Mit der bewährten Anti-Exploit-Technologie von Sophos Intercept X stoppen Sie Exploits, bevor es zu spät ist. Diese Next-Gen-Endpoint-Lösung ergänzt Ihre bestehende Antivirus-Software und ermöglicht Ihnen, Ihr Unternehmen mit minimalem Aufwand zu schützen.

## Weitere Informationen

Nähere Informationen über CVE-2012-0158 erhalten Sie in dem detaillierten technischen Report von den SophosLabs.

**Testen Sie Sophos Intercept X kostenfrei: www.sophos.de/intercept-x**

Sales DACH (Deutschland, Österreich, Schweiz):
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

© Copyright 2016. Sophos Ltd. Alle Rechte vorbehalten.
Eingetragen in England und Wales, Nr. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, GB
Sophos ist die eingetragene Marke von Sophos Ltd. Alle anderen genannten Produkt- und Unternehmensnamen sind Marken oder eingetragene Marken ihres jeweiligen Inhabers.

16-09-13 WPDE (RP)

SOPHOS