Verlagsbeilage, August 2012

‹kes›
Die Zeitschrift für Informations-Sicherheit

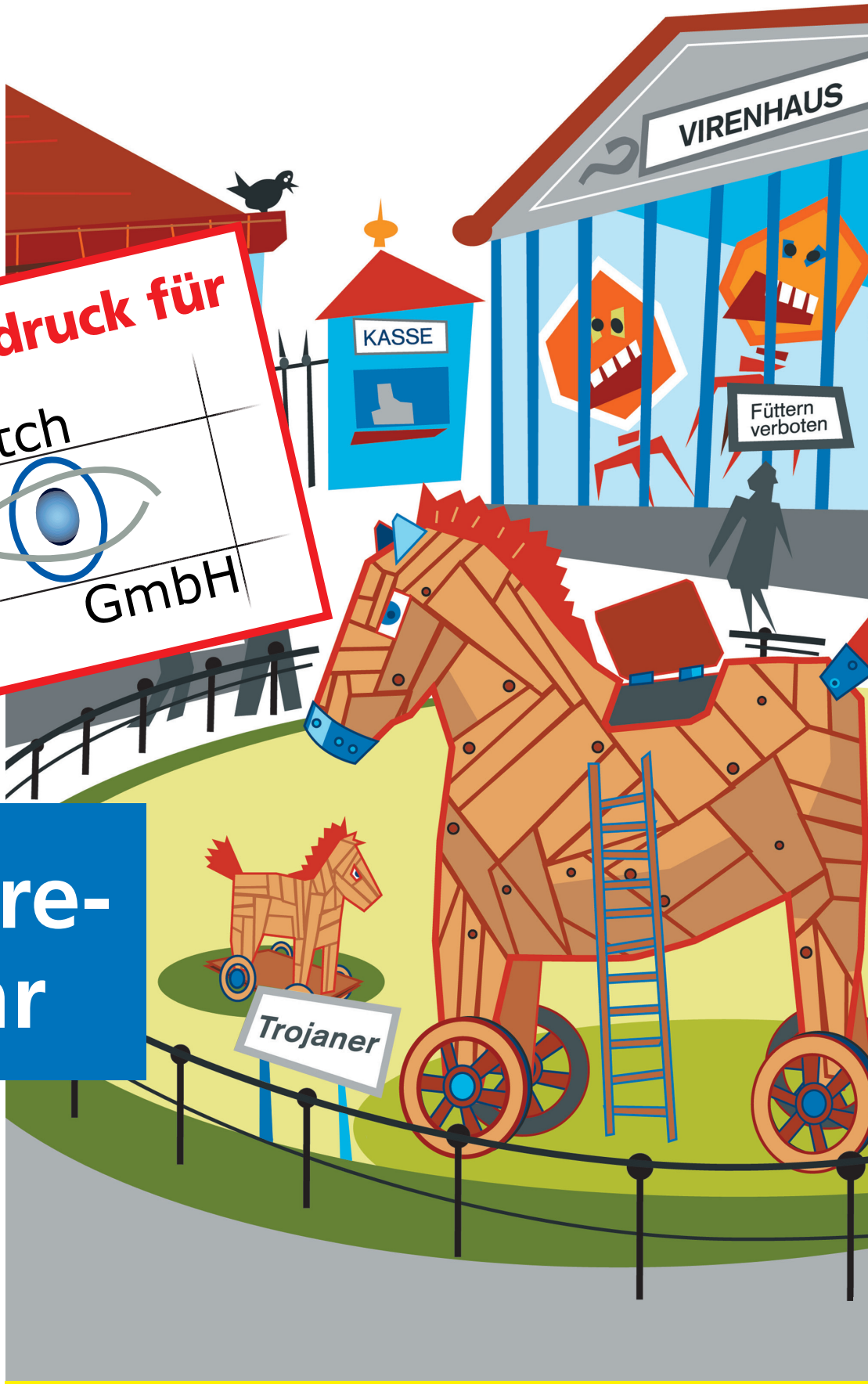
special

IT·Grundschutz Informationsdienst

WIK Zeitschrift für die Sicherheit der Wirtschaft

Sonderdruck für itWatch GmbH

Malware-Abwehr



SecuMedia

Mit ReCoBS gegen Drive-by-Downloads S.16

Stand der Technik

White-/Blacklisting allein ist chancenlos

Eine Fülle von nationalen und internationalen Bestimmungen definieren die Compliance-Anforderungen in Unternehmen – der Schutz vor Malware gehört hier nicht nur entlang des Bundesdatenschutzgesetzes dazu. Hinzu kommen auch weitere wie KonTraG, SOX, HIPPA, Basel II, GOBS, FAMA, TDDG, Euro Sox, deren Vorschriften bestimmte Branchen oder den gesamten IT-Markt betreffen. Ein guter Schutz vor Malware ist heute durch traditionelle Ansätze des White- und Blacklisting nicht mehr erreichbar. Ein oder besser zwei gute Anti-Viren-Lösungen sind Grundvoraussetzung, aber was müssen Unternehmen noch tun?

Von Dipl. Inform. Ramon Mörl, itWatch GmbH

Etwa um das Jahr 2004/2005 wurde im Markt allen bewusst, dass neue technische Wege in der Bekämpfung von Malware beschritten werden müssen. Patternbasierte Malwareerkennung half zwar gegen das Grundrauschen, aber intelligente Angriffe blieben unentdeckt und mussten dann teuer von den befallenen Systemen entsorgt werden. Grund dafür waren vor allem sich selbst verändernde Angriffscodes, zielgerichtete Attacken in unterschiedlichster Ausprägung, die im professionellen Fall oft mit „social engineering"-Attacken kombiniert wurden, und natürlich in „guten" Objekten versteckte Angriffe.

Mit White- oder Blacklisting faule Eier suchen ist chancenlos

In dieser Zeit wurde dann der Versuch unternommen, die kritischen Daten eines Systems zu schützen und mit den bekannten Werkzeugen White- und Blacklisting auf Anwendungs- und Prozessebene gegen Angriffe vorzugehen. Dies verursachte jedoch Probleme: Viele selbst entwickelte Anwendungen wurden fälschlicherweise als Angreifer identifiziert, die Nutzer waren (daher) unzufrieden und Steuerungsmechanismen, wie das Aufnehmen einer selbst implementierten Anwendung in eine Whitelist, waren noch sehr rudimentär implementiert. Die herkömmlichen Maßnahmen White- und Blacklisting stießen also an ihre Grenzen. Als Lösung wurden schließlich heuristische Methoden hoch gehandelt, um die neuen Feinde zu bekämpfen, bargen jedoch zu große Fehlerquellen, denn „gute" Daten wurden auf einmal abgewiesen, bloß weil sie neue Formate hatten. Außerdem lernten die Angreifer schnell, dass man heuristische Verfahren durch andere „Verstecke" aushebeln konnte.

Schwarz-Weiß gedacht

Eine Whitelist ist eine Policy, die alles verbietet, bis auf die Elemente, die explizit freigegeben sind. Unter einer Blacklist versteht man eine generelle Freigabe (alles erlaubt) und individuelle Sperre von einzelnen Elementen. Für gutes Whitelisting ist es also notwendig, alle „Guten" auf die weiße Liste zu schreiben. Das ist aber leider zu kurz gedacht, denn wenn man die „Guten" nicht wirklich sicher identifizieren kann, dann können die „Bösen" trotz weißer Liste einfach teilnehmen. Ein Beispiel: Hat ein Unternehmen ein Device-Control-System eingerichtet, das einen sicheren USB-Stick anhand des Namens identifiziert und allen anderen USB-Sticks den Zugriff verweigert, dann genügt es oft, einen Memory-Stick entsprechend umzubenennen und die Daten werden auf diesen unverschlüsselt ausgelagert – ohne dass der Anwender es merkt. Es gilt also, die Kandidaten auf der weißen Liste zu authentisieren. Im Fall von USB-Sticks geht das mit den geeigneten Werkzeugen recht einfach durch eine Individualisierung des Sticks, eine Personalisierung oder sogar ein vollständiges starkes Authentisierungsprotokoll.

In der IT-Welt gibt es jedoch nicht nur sicherheitsrelevante Geräte, deren eindeutige authentisierte Charakteristik Voraussetzung zum Einsatz ist, sondern auch – auf den ersten Blick – völlig belanglose „Massenware". Zu diesen zählen Mäuse, Drucker, HID, CPU, Monitor. Hier steht nicht die Sicherheit im Vordergrund, sondern das einfache Management. Es sollte daher möglich sein, erst einmal alle diese Geräte freizugeben und nur die schwarzen Schafe zu sperren. Das ist ein sinnvoller Einsatz für das Blacklisting-Verfahren. Der Grund, eine Maus zu sperren, könnte sein, dass dieser Typ wegen Treiberproblemen an bestimmten Rechnern nicht richtig funktioniert – also eher keine Sicherheitsgründe.

Die Kenntnis und insbesondere die Pflege von Policy-Elementen, inklusive der Authentisierung des individuellen Elements, sollten deshalb nur bei sensiblen oder schutzbedürftigen Technologien notwendig sein. Das Unternehmen selbst muss die Entscheidung treffen können, welche Technologien als schutzbedürftig gelten. Bei diesen wird ein Whitelist-Ansatz das Mittel der Wahl sein, um nur bekannte und unternehmenseigene Elemente für Berechtigte zuzulassen. So wird die Komplexität der Policy durch das Unternehmen selbst bestimmt und damit auch der Aufwand, der in die Administration fließt. Der subjektiv definierte Schutzbedarf wird bei jeder Technologie unternehmensindividuell berücksichtigt – das spart Kosten in der Administration.

Der generelle Vorteil dieser Art der Umsetzung besteht darin, dass die IT-Security-Policy eines Unternehmens nur so komplex wird, wie es für die individuell gestellten Anforderungen unerlässlich ist. So kostet die Freigabe einer ganzen Klasse von unkritischen Objekten (Devices, Anwendungen, Zugriffsarten, Dokumente) nur ein einziges Policy-Element, unabhängig davon, wie viele unterschiedliche Instanzen von diesem Objekttyp im Unternehmen vorhanden sind (Blacklist).

Sicher gegen Malware – erfolgreiche Ansätze

Die Netzwerkkontaktpunkte sind heute über Firewall-Systeme meist gut gegen Malware geschützt, dürfen aber aus rechtlichen Gründen häufig die verschlüsselten Datenströme nicht „aufbrechen". Der Schutz vor Malware muss deshalb zwingend auf die Endpunkte, die PCs und Notebooks erweitert werden. Zudem können die Daten auf dem Endpunkt besonders einfach geprüft werden. Hier liegen sie zum einen unverschlüsselt und ohne Komprimierung vor, zum anderen ist der Handlungskontext des Anwenders genau bekannt.

Ist-Zustand kennen

Wichtig ist, potenziell kritische Punkte zu identifizieren, die als Eintrittspunkte für Angriffe dienen können. Es geht dabei um Netzwerkübergänge zwischen privaten und öffentlichen Netzen, Kommunikationsanwendungen wie Browser und E-Mail, Ports / Schnittstellen, Geräte wie Modems, Netzwerkkarten oder auch mobile Datenträger wie Memory Sticks, gebrannte DVDs oder externe Festplatten. Ein Software-gestütztes Risikomonitoring all dieser Angriffspunkte bezüglich der Verwendung der Geräte, Schnittstellen und Ports, Netzverbindungen, der Anwendungen (welche sind

wann und ggf. von wem im Einsatz und was tun sie) sowie der Dateneingang und -ausgang ergibt ein umfassendes Bild über den Ist-Zustand der Sicherheit und der Bedrohungen. Die Monitoring-Ergebnisse dienen dazu, das gültige Sicherheitskonzept zu verfeinern und der aktuellen Situation anzupassen. Ebenso dienen die Risiko-Reports später dazu, die Verbesserung messbar zu machen oder bestimmte problematische Datenbewegungen forensisch zu bearbeiten.

Grundpfeiler Pattern-Analyse

Word-, Powerpoint, rtf und PDF-Dokumente stehen laut den Berichten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) auf der Hitliste der populärsten Formate für eingebettete Angriffe weit oben. Diese Objekte können Schadcode als eingebettete ausführbare Programme enthalten. Eine gute Pattern-Analyse kann durch eine intelligente Inhaltsüberprüfung diese eingebetteten Programme in Echtzeit vor der Ausführung erkennen und je nach Notwendigkeit durch Verbot, Quarantäne oder Ausführung in einer Sandbox oder virtualisierten Umgebung (z. B. ReCAppS) reagieren. Damit der Schutz vollständig ist, muss das Sicherheitskonzept in der Lage sein, auch in beliebig geschachtelten Archiven oder verschlüsselten Dateien nach diesen Mustern zu suchen. Dieses Verfahren ist ein wesentlicher Grundpfeiler – reicht aber immer noch nicht aus.

Rechte und Isolation

Eine wirksame Maßnahme gegen die verbleibenden Restrisiken durch Schadcode ist durch zwei weitere Verfahren gegeben: Rechte für Anwendungen und Isolation durch (virtuelle) Schleusen. Drive-by-Attacken bringen den Browser dazu, Malware im Rechteraum des Anwenders auszuführen. Hat der Anwender das Recht JavaScript auszuführen, DLLs zu schreiben oder sogar bestehende zu ersetzen oder beliebige neue Executables in das System einzubringen, wird die Drive-by-Attacke ohne weitere Schutzmaßnahme erfolgreich sein. Kann man aber in seiner Endgeräte-Sicherheitsrichtlinie einfach der Anwendung das Recht nehmen, DLLs zu schreiben, JavaScript auszuführen oder Executables zu starten, dann ist das Ziel erreicht, ohne den Anwender in seinen Rechten zu beschneiden.

Genauso elegant kann man die Anwendung, die diese problematische Aktion ausführen möchte, in einer Schleuse ausführen. Schleusenrechner sind noch allseits bekannt und aufgrund der „Wegstrecke“ durch die physikalische Trennung von Netz und Arbeitsplatz unbeliebt. Die Schleusenfunktion kann aber auch lokal, zentral oder in der Cloud erbracht werden, ohne vom Arbeitsplatz aufzustehen – also virtualisiert werden und jeweils mit unterschiedlichen Mechanismen von den produktiven Netzen getrennt werden. Negativ wirken sich alle Schleusenlösungen aus, die den Datenfluss zwischen virtuellem Sandkasten und produktiven System zwangsweise vollständig verhindern. Real muss dieser Datenfluss für die geeignete Einbindung (z.B. das Drucken) mit den geeigneten Mechanismen, also Automatisierung und Inhaltsüberprüfung, ausgestattet sein. Das heißt, der Schutz vor Malware über virtuelle Schleusen impliziert wieder die Anbindung der virtuellen Schleuse – ähnlich als wäre ein externer Datenträger angesteckt – zur weiteren praktischen Verwendung, aber eben mit sicheren Protokollen und Datenaustausch. Druckdatenströme können nicht auf Application Level auf einer Firewall untersucht werden – gute Produkte lösen diese Herausforderung aber sicher.

Als entscheidender Faktor kommt letztlich die Unternehmenskultur hinzu, denn im Umsetzen der Aufgabenstellung wird das Unternehmen sich entscheiden, ob der Anwender vor lauter Sicherheit nicht mehr arbeiten kann (IT-Sicherheit als Arbeitsverhinderer) oder die Sicherheit hinten angestellt ist, weil die Anwender all die neuen Anwendungen und Möglichkeiten in der Cloud brauchen. Oder es wird die Infrastruktur so zur Verfügung gestellt, dass der Anwender alles tun kann, aber immer sicher handelt. In der Praxis heißt das je nach dem angemeldeten Benutzer und der durchgeführten Aktion, die richtige Lösung zwischen dem „selbstverantwortlichen Benutzer“ mit allen Freiräumen und dem möglicherweise ungeschulten „Normalnutzer“ jeweils situationsabhängig zu finden und vorab in einer flexiblen technischen Sicherheitsrichtlinie zu verankern, die immer technisch durchgesetzt wird.

Fazit

Zum wirklichen Schutz vor Malware genügen die Ansätze der Whitelists schon lange nicht mehr. Weitere Verfahren sind notwendig und im Markt seit Jahren verfügbar. Nur wenige Anbieter verfeinern das technische Angebot regelmäßig weiter, sodass gegen neue noch unbekannte Angriffe bereits geeigneter Schutz geboten wird. Die vergangenen 15 Jahre zeigen, dass hier die deutschen Sicherheitsarchitekten bereits vor DMA, Conficker, stuxnet, duqu und Flame Lösungen erarbeitet hatten, die ohne genaue Kenntnis des Angriffs trotzdem vor diesem schützen konnten.