STORMSHIELD

DIE VISION:

INEINANDERGREIFENDE IT-SICHERHEIT AUF MEHREREN EBENEN

MULTILAYER COLLABORATIVE SECURITY

SCHUTZSYSTEME SO KOORDINIEREN,
DASS SIE DAS GESAMTE SICHERHEITSNIVEAU ANHEBEN
UND DEN MEISTEN RAFFINIERTEN ATTACKEN STANDHALTEN

Whitepaper

NETWORK SECURITY | ENDPOINT SECURITY | DATA SECURITY

Weil sie schwer zu erkennen sind, erfordern **die aktuellen fortschrittlichen Angriffe einen mehrschichtigen Schutz**. Aus diesem Grund müssen unternehmensweit eingesetzte Sicherheitslösungen gewissenhaft integriert und koordiniert werden.

Attacken, die sich gegen Netzwerke richten, werden immer ausgefeilter und schwerer zu erkennen. Diese höchst unauffälligen Bedrohungen kombinieren mehrere Angriffsvektoren miteinander, um ihre Ziele zu erreichen.

Sobald ein Opfer identifiziert wurde, starten solche Angriffe oft mit einem harmlos aussehenden Vektor. Zu diesem Zeitpunkt realisieren die Betroffenen noch nicht, dass sie im Visier einer Attacke stehen, die das vorhandene Schutzsystem überhaupt nicht erkannt hat. Der Angriff wird sich dann mittels verschieden ausgeprägter und erfolgreicher Techniken zum angepeilten Netzwerk hin verbreiten, um das definierte Ziel zu erreichen (Serverbeschädigung, Datenausschleusung etc.). Der Zeitraum zwischen dem Beginn des Angriffs und der Erreichung des Ziels zählt zu den wesentlichen Merkmalen von **APTs (Advanced Persistent Threats).**

KOORDINIERTER SCHUTZ

Diese fortschrittlichen Angriffe sind so konzipiert, dass sie konventionelle Schutzsysteme umgehen können. Die Kombination mehrerer Security-Lösungen in Form von Silos ist keinesfalls effektiv genug. Allerdings hinterlassen die Attacken Spuren, die als schwache Anzeichen gedeutet werden können, wie z.B. als Zugriff auf eine nicht kategorisierte Website.

Durch die Verbindung dieser schwachen Signale miteinander und ihrer Korrelation in einer Schwachstellenkarte kann eine Bedrohung identifiziert und ihre wahrhaftige kritische Natur enthüllt werden. **Daher kann Multilevel-Angriffen durch Anordnung mehrerer Schutzschichten, die miteinander interagieren, begegnet werden.**

In der Praxis lässt sich dies auf zwei verschiedene Weisen umsetzen. Die erste Option ist, Events mittels SIEM (Security Incident and Event Management)-Lösungen zu korrelieren. Sicherheitsvorfälle werden gesammelt und anschließend analysiert, um abnormales Verhalten zu erkennen. Jedoch können Vorfälle erst dann korreliert werden, wenn sie eingetreten sind. Der Administrator kann lediglich reaktiv auf die Sicherheitsvorgaben agieren.

Als zweite Option – mit einer Vorgehensweise, die auf der Integration von Security Engines und Interaktion zwischen den verschiedenen Abwehrlösungen basiert – kooperieren die unterschiedlichen Schutzmechanismen miteinander, um Daten auszutauschen und Verhaltensweisen zu analysieren, die bei anderen Vorfällen identifiziert wurden. **Die Korrelation findet in Echtzeit statt, und die verschiedenen schwachen Signale werden weltweit berücksichtigt.** Auf diese Weise wird das Schutzniveau gestärkt, während sich die Security Policy dynamisch anpassen lässt. Unnormales Verhalten kann somit schneller abgeblockt werden – sogar auf proaktive Weise.

Diese Vorgehensweise ist die Grundlage der Stormshield-Vision, wie neuen Bedrohungen begegnet werden sollte.

INHALTSVERZEICHNIS

Fortschrittliche Attacken erkennen

Sofern sie gewissenhaft vorbereitet werden, nutzen fortschrittliche Attacken Schwachstellen aus, um sich ihren Weg ins interne Netzwerk zu bahnen, dort neue Ziele anzuvisieren und dann **kritische Services abzuschalten oder vertrauliche Daten zu stehlen**.

EINE UMGEBUNG, OFFEN FÜR ANGREIFBARE PLATTFORMEN

Innerhalb von drei Jahrzehnten hat sich die digitale Landschaft vollkommen gewandelt: IT ist zu einer Handelsware geworden, während PCs, Smartphones und Touchscreen-Tablets die Gewohnheiten von privaten wie beruflichen Nutzern verändert haben. Das Internet und die sozialen Netzwerke haben zudem die Art, wie wir kommunizieren und arbeiten, revolutioniert. Informationen zu erstellen und miteinander zu teilen war noch nie so einfach – jeder kann Inhalte verbreiten und mit seiner Umgebungen interagieren.

Diese offene, stets verbundene Umgebung bietet ideale Chancen für den Missbrauch. Weil die User über die Jahre vorsichtiger geworden sind, müssen Hacker ausgefeiltere Techniken finden, um ihre Ziele zu erreichen. Mittlerweile nutzen sie Schwachstellen auf legitimierten Websites oder in E-Mail-Anhängen aus, um die Arbeitsplätze der Benutzer zu identifizieren, die die Seiten oder Nachrichten öffnen. Der von Hackern eingesetzte bösartige Code nutzt oftmals Zero-Day-Lücken aus, insbesondere solche in Anwendungen, die häufig zum Lesen von Dokumenten oder Web Content verwendet werden.

Täglich werden neue Websites besetzt, mit dem Ziel, verseuchten Code zu injizieren und dort zu hosten. Dieser Code macht sich die zahlreichen Schwachstellen zunutze, die sich in Webbrowsern und den damit verbundenen Komponenten finden (wie Flash oder Java), um die Computerarbeitsplätze von Internetnutzern zu kompromittieren.

Verbesserte Angriffstechniken berücksichtigen auch die Weiterentwicklung der Schutzmethoden. Das aktuelle Prinzip vertraut entweder auf gänzlich unbekannten Schadcode oder die Kombination verschiedener Methoden, die sich durch die eingerichteten Filter schleichen können.

EINE GUT STRUKTURIERTE BEDROHUNG

Cybercrime ist zu einer eigenen Wirtschaft im Untergrund herangewachsen und verfügt über Organisationen, dedizierte Finanzquellen und Währungen. Die Ziele von Internetkriminalität variieren:

- Cyber-Kriegsführung (Warfare), politische Destabilisierung, Spionage im Auftrag von staatlichen Organisationen,

- politisch oder ideologisch motivierter Aktivismus (bsp. Anonymous oder Lultsec),
- finanzielle Gewinne (Lösegeld, Erpressung, Datendiebstahl oder -wiederverkauf, Hacking- oder Angriffs-„Services"),

Cyberkriminalität ist oftmals gut vorbereitet, sodass Angriffe effizient und gezielt gestartet werden können. Um eine bösartige Kampagne erfolgreich durchzuführen, werden der Zweck und das Ziel mit Bedacht ausgewählt.

Die Tabelle 1 zeigt, wie APT willkürlich Regierungsministerien, Zeitungen, IT-Unternehmen sowie die Energie- und Freizeitbranche attackieren:

Bezeichnung	Jahr	Vektor	Zweck	Ziel	Vermuteter Ursprung
Stuxnet	2008	USB-Schlüssel und Wurm, der ein Industriekontroll-system von Siemens angriff	Industriesabotage durch die Infizierung von Zentrifugen	Atomindustrie im Iran	USA und Israel
Operation Aurora	2009	Zero-Day-Schwach-stellen und Backdoor	Diebstahl des Quellcodes von innovativen multinationalen Unternehmen	Quellcode-datenbestände von Adobe, Google, Juniper, Rackspace etc.	China
Bercy (Französisches Wirtschafts-, Finanz- und Industrie-ministerium)	2010	PDF-Anhang mit Trojaner	Informationen zu G20 sammeln	150 infizierte Systeme	Asien
RSA	2011	HTran-Malware	Informations-diebstahl betreffend SecurID-Tokens	Netzwerk des Security-Zweigs der EMC Group	China
New York Times	2013	Spear-Phishing-Attacke: E-Mails mit verseuchten Links	Diebstahl von Passwörtern und Dateien der Journalisten	Die Büros	China
Sony Pictures	2014	Wahrscheinlich Spear-Phishing mit einem Trojaner und Ransomware	Zerstörung von Dateien, Diebstahl von vertrauli-chen Daten und unveröffentlich-ten Filmen	Produktionsserver der Studios	Nordkorea

Tabelle 1
Einige bekannte APT-Angriffe seit 2008

NIEMAND BLEIBT VERSCHONT

Cyberkriminalität in all ihren Ausprägungen macht sich die Vernetzung der Informationssysteme in Unternehmen jeder Größe zunutze, die in IT-Ökosystemen angelegt sind. Infolgedessen bleiben kein Zulieferer, kein Wirtschafts- und kein Technologiepartner verschont.

Um der Erkennung durch das anvisierte Unternehmen zu entgehen, vertraut ein Hacker auf die IT-Netzwerke, die zwischen kleinen und mittelgroßen Firmen gespannt sind, die in vollstem Vertrauen miteinander arbeiten. Durch die Kompromittierung eines Hosts im Netzwerk des Partners oder eines Subunternehmers wird das komplette Ökosystem gefährdet.

Angesichts der unterschiedlichen Gründe hinter Internetkriminalität sind auch die kleinsten Organisationen besorgt. Tatsächlich sind sowohl die finanziellen Informationen über die Kunden einer Steuerberatungsfirma und die Patienteninformationen eines medizinischen Zentrums als auch die Betriebsgeheimnisse einer Forschungseinheit Beispiele für schützenswerte Daten. Darüber hinaus kann ein Sicherheitsvorfall im Informationssystem einer kleinen Organisation kurzerhand zur Stilllegung ihrer Aktivität führen, da sie in großen Umfang auf den Einsatz von Computertools vertraut.

EINE ONLINE-DATEN-GOLDMINE

Die zahlenmäßige Explosion der sozialen Netzwerke hat es so viel einfacher gemacht, Informationen über ein Opfer zu sammeln und die Chance auf einen erfolgreichen Hacking-Angriff zu erhöhen. Sobald ein Unternehmen als Ziel ausgewählt wurde und der Zweck festgelegt ist, wird der Hacker damit beginnen, das Opfer der ersten Attacke zu identifizieren. Dabei handelt es sich meist um einen Mitarbeiter, der in sozialen Netzwerken aktiv ist. Das Ziel dieser Taktik ist es, einen Weg auszuarbeiten, den anvisierten Mitarbeiter zu täuschen.

Diese Phase des Social Engineering-Plans ermöglicht es, den Angriffsvektor zu erkennen, wie z.B. eine E-Mail mit gezieltem Inhalt oder ein USB-Schlüssel, der absichtlich an einem Ort hinterlegt wird, den das Opfer häufig aufsucht.

DIE DREI PHASEN EINES APT

Die ausgefeiltesten Bedrohungen werden mittels eines APT (Advanced Persistent Threat) übertragen. Der sehr zielgerichtet arbeitende APT vereint mehrere Angriffsvektoren und wird in drei Phasen ausgeführt, um unbemerkt zu bleiben. Ein APT wird vorbereitet, indem das zu treffende Unternehmen und sein erstes Opfer ausgewählt werden. Ein Social Engineering Exploit bestimmt den idealen Vektor für den ersten Angriff, um die Erfolgschancen zu erhöhen. Dann startet die Attacke mit einer ersten Infizierung, die sich die Schwachstellen von Anwendungen zunutze

macht, die am Computerarbeitsplatz (Workstation) des Opfers installiert sind. Der Angriffsvektor – eine E-Mail oder ein USB-Schlüssel – enthält entweder ein speziell angefertigtes Dokument oder einen Link zu einer verseuchten Website.

Sobald der Computerarbeitsplatz des Opfers infiziert wurde, fokussiert sich die folgende Expansionsphase darauf, den Host oder sogar die anvisierten Daten zu erreichen. Die erste Viruslast kann modifiziert sein, um einen Command-and-Control-Channel aufzusetzen und andere Maschinen, die mit dem Netzwerk verbunden sind, zu infizieren. Zuletzt wird der APT in die dritte Phase übergehen, um die definierte Handlung auszuführen. Zu diesem Zeitpunkt wird der Angriff aktiv und schaltet den Server ab oder stiehlt vertrauliche Informationen. Wenn ein abgeschalteter Server schnellstmöglich anzeigt, dass eine Attacke stattgefunden hat, kann das Datenleck sukzessive auftreten – die Attacke würde dann andauern und unerkennbar dort verbleiben.

Beispiel: ein Mitarbeiter, der für Frachtaufträge verantwortlich ist. Mittels Social Engineering wäre es möglich, den Arbeitsplatz des Opfers und den Namen des regulären Logistikträgers ausfindig zu machen. Um den Mitarbeiter glauben zu machen, er lese eine offizielle Nachricht, wird eine verseuchte E-Mail die Identität des Logistikunternehmens imitieren und einen plausiblen Anhang erhalten, wie z.B. ein Auftragsformular:

PHASE 1: PRIMÄRINFEKTION

Schadcode nutzt Schwachstellen aus, die in gewöhnlichen Anwendungen wie Webbrowsern und Bürokommunikationsmitteln (Office, PDF) vorkommen. Lücken in Browsern und ihren Software-Bestandteilen sind ein begehrtes Ziel: Eine von drei Web-Attacken missbraucht auf diese Weise Java Plugins.

Eine andere Möglichkeit, verseuchten Code zu transportieren, ist per E-Mail-Anhang. Das Opfer öffnet ein angehängtes Dokument oder besucht eine korrumpierte Website und installiert dabei ungewollt den Schadcode. Da der Installationsprozess ohne jegliches Anzeichen oder Vorfälle vonstattengeht, ahnt das Opfer nichts.

In Bezug auf das Beispiel bedeutet das: Der Logistikmitarbeiter würde annehmen, dass er ein gewöhnliches Auftragsformular öffnet. Sobald das Dokument geöffnet ist, wird eine Lücke im System ausgenutzt, um heimlich bösartigen Code zu installieren.

PHASE 2: EXPANSION

Die Primärinfektion schafft den Eintrittspunkt für den APT, der anschließend versucht, sich im anvisierten Unternehmen zu verbreiten. Der APT kombiniert mehrere Vektoren, um verschiedene Ankerpunkte ausfindig zu machen und die Zielsetzung zu erreichen. Allgemein werden diese Ankerpunkte initiiert, indem ein

Command-and-Control-Channel zwischen dem Hacker und den kompromittierten Hosts aufgebaut wird. Diese Technik ermöglicht es dem Hacker, das Verhalten der verseuchten Ladung remote zu verändern. Auf diesem Weg setzt der infizierte Host eine legitime Verbindung zu einem unbekannten Command-and-Control-Server auf. Die Expansionsphase findet simultan an zwei Fokuspunkten statt:

- Die verseuchte „Lieferung“ wird durch den Command-and-Control-Channel transformiert. Die Technik kann die Malware upgraden, indem sie Funktionen hinzufügt, sodass sie das anvisierte Unternehmen noch effizienter penetrieren kann. Der Channel kann auch versuchen, Rechte zu erweitern oder willkürlichen Code auszuführen, um Netzwerkverbindungen auf anderen Hosts einzurichten oder sogar eine Authentifizierungsphase zu wiederholen..
- Die Anzahl der infizierten Hosts steigt: Der Schadcode oder der unbekannte Command-and-Control-Channel agieren als Vermittler, um nach neuen verwundbaren Hosts zu suchen. Diese Phase kombiniert verschiedene Angriffsvektoren und trachtet danach, weitere Hosts, die möglicherweise weniger gut geschützt sind, zu kompromittieren.

Mit der Verbreitung der Attacke wird bezweckt, dass das Ziel – ein Server für Finanztransaktionen oder eine Datenbank – im Voraus erreicht wird. Sobald das Ziel lokalisiert ist, geht der APT in die finale Phase. Erst dann wird der Angriff tatsächlich aktiv und erkennbar – aber nur in bestimmten Fällen.

PHASE 3:
DATENKOMPROMITTIERUNG ODER -DIEBSTAHL

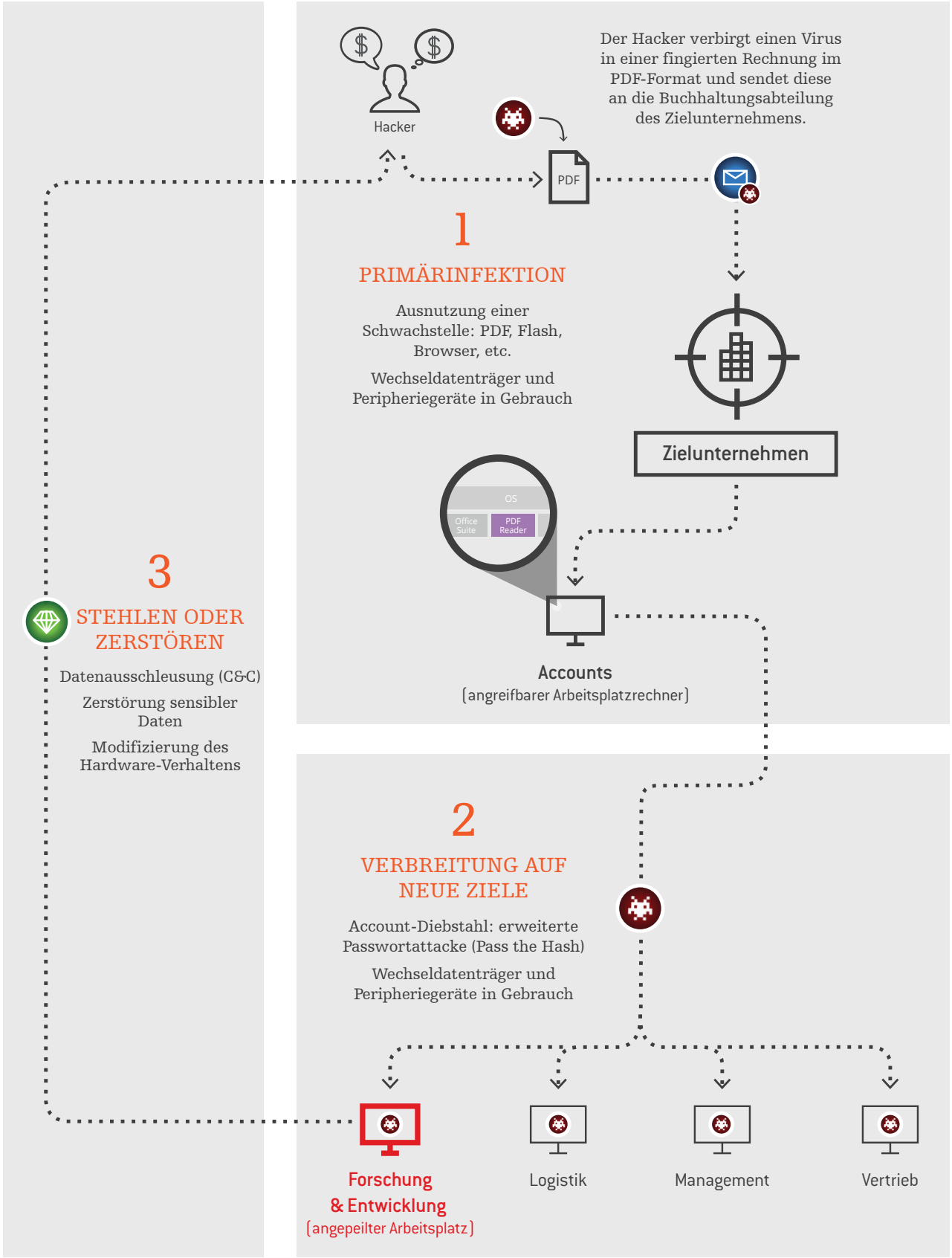
Diese Phase eines APT greift die gewählte Plattform mit einem speziellen Ziel an. Das kann ein PC in der Personalabteilung sein, an dem Gehaltszettel ausgestellt werden, ein Arbeitsplatz in der Supply-Chain-Abteilung oder auch ein Server für E-Commerce oder Finanztransaktionen. Der Angreifer hat seine Attacke vorbereitet, zum Beispiel, indem er einen Onlineserver stoppt, um Lösegeld zu fordern, bevor er ihn wieder anlaufen lässt, oder indem er vertrauliche Informationen für den Weiterverkauf extrahiert. Zur Verdeutlichung dieses Punkts: Im Juni 2014 wurde die US-amerikanische Kette Domino’s Pizza aufgefordert, 30.000 Euro zu bezahlen, nachdem persönliche Informationen von 600.000 Kunden gestohlen worden waren.

Im Falle eines kompromittierten Servers zeigt die Ausführung einer Attacke auch das Vorkommen von Schadcode innerhalb des anvisierten Unternehmens an. Dennoch kann er nicht direkt nach seiner Enthüllung komplett ausgemerzt werden. Der Server kann wiederhergestellt werden, bis sich der Hacker dafür entscheidet, den Schadcode nochmals zu nutzen, erneut Lösegeld zu verlangen oder remote Dateien zu zerstören.

Im Falle eines ausreichend diskreten Datenlecks muss die APT-Attacke nicht unbedingt erkannt werden. Der Angriff kann somit für mehrere Monate oder sogar Jahre weiter vertrauliche Informationen abschöpfen.

Schema einer komplexen Cyber-Attacke

Wie fortschrittliche Angriffe ablaufen



Wählen Sie mehrschichtigen Schutz

Die in einem Unternehmensnetzwerk eingesetzten Schutzlösungen müssen Informationen zum Verhalten austauschen, die sowohl untereinander als auch auf globaler Ebene beobachtet wurden. Nur so ist man auf die nächste Attacke vorbereitet.

DIE GRENZEN VON SILO-SCHUTZSYSTEMEN

Sobald herkömmliche Schutzmechanismen (Antivirus, IPS, HIPS, URL-Filter etc.) von immer raffinierteren Bedrohungen „löchrig gefressen" werden, verringern sie zwar die Angriffsfläche für eine Attacke, stoßen jedoch im weiteren Verlauf an ihre Grenzen. Die Kombination mehrerer Angriffsvektoren und APT-Belastungen erhöht das Risiko. Da Malware-Code nicht direkt durch Primärinfektionen der APTs aktiviert wird, nutzt er System- oder Applikationsschwachstellen, um den Zielcomputer zu lokalisieren und anschließend zu kontrollieren

Die Malware, die die Anfälligkeit einer Office-Anwendung nutzt, hat oftmals keine Auswirkungen auf den Betrieb eines Arbeitsplatzrechners. Alternativ würde allerdings eine HTTP-Verbindung zu einem Command-and-Control-Server hergestellt, um so neuen Malware-Code zu aktivieren. Da entsprechende Attacken oft nicht als echte Bedrohungen erkannt werden, werden sie auch nicht von herkömmlichen Schutzlösungen blockiert. Solche Angriffe sind meist speziell geplant, so dass ihnen signaturbasierende Sicherheitssysteme nicht auf die Schliche kommen.

Die Bedrohung wird erst dann Realität, wenn die Primärinfektion das Unternehmensnetzwerk umfangreicher befällt: Bei einer Zero-Day-Bedrohung z.B. erhöht sich der Risikograd, wenn sich der Angriff verbreitet. Solch fortschrittliche Attacken hinterlassen jedoch Spuren (Verbindung zu einer Webseite, die nicht vom Web-Filter betroffen ist; Benachrichtigungen bei der Erfassung interaktiver Verbindungen oder misstrauisch betrachteter interner Verbindungen), die als schwache Signale aufgefangen werden.

Eine wirkliche Bedrohung wird deutlich, wenn verschiedene, einzeln betrachtet scheinbar harmlose Ereignisse korrelieren. Daher sind die schwachen Signale bzw. deren Kontext überaus wichtig für das Identifizieren oder Blockieren von APTs.

VORFÄLLE KORRELIEREN

Ein Gesamtüberblick von Sicherheitsereignissen im Unternehmensnetzwerk liefert Informationen darüber, in welcher Form die Advanced Persistent-Attacke stattgefunden hat. Diverse Formen von verdächtigem Verhalten und schwachen Signalen tauchen meist an einem zentralen Punkt auf, was die Erkennung einer Multivektor-Bedrohung erleichtert. Die Analyse verschiedener Sicherheitsereignisse würde es ermöglichen, jede Bedrohung einzeln und aufgrund abnormaler Verhaltensmuster zu identifizieren. Ansonsten würde die Erkennung eines APT

eine zusätzliche Analyse erfordern.

Die Anwendung der Ereigniskorrelation erleichtert die Analyse, da z.B. plötzliche Anstiege in der Anzahl der Verbindungen von einem bestimmten Host zu einer bestimmten Zeit oder Verbindungen zu ungewöhnlichen Services, Ressourcen etc. hervorgehoben würden.

Auf diese Weise bietet die Assoziation individueller Vorfälle kontextbezogene Einblicke, durch die eine Advanced Persistent-Attacke aufgedeckt werden kann.

DER MEHRSCHICHTIGE (MULTILAYER-)ANSATZ

Die Analyse korrelierter Ereignisse erlaubt nur das Reagieren auf eine fortschrittliche Attacke. Daher muss ein proaktiver Ansatz eingerichtet werden: zum einen, um das Schutzniveau zu erhöhen, und zum anderen, um zu verhindern, dass Mitarbeiterteams unter Netzwerküberlastungen leiden. Das Prinzip dieses Ansatzes ergibt sich aus der Zusammenarbeit verschiedener Schutzmethoden, verteilt über drei Schichten:

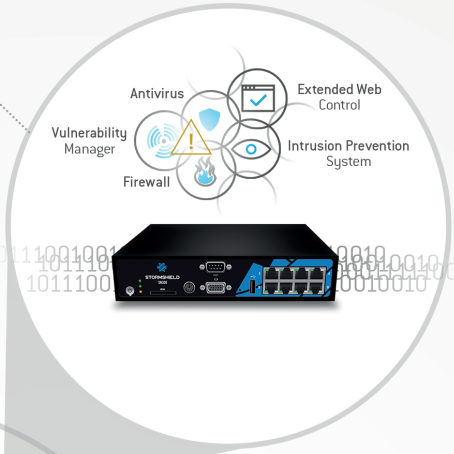
- **Schicht 1 – Gemeinschaftlicher Schutz:** Die zu einem System (Multifunktionsfirewall oder Workstation-Schutz) gehörenden Protection Engines tauschen Informationen über beobachtete geringe Signale aus, um schädliches Verhalten zu erkennen und zu blockieren.
- **Schicht 2 – Kontextabhängiger Schutz:** Die verschiedenen Sicherheitslösungen des Informationssystems arbeiten zusammen, um Infos über schwache Signale auszutauschen, neues unerlaubtes Verhalten zu identifizieren und um eine aufeinander abgestimmte Reaktion auf Malware und Co. zu geben.
- **Schicht 3 – Globaler Schutz:** Alle Schutzlösungen, die in mehreren Organisationen eingesetzt werden, halten Informationen fest, die zusammengefasst einen globalen Überblick über alle Bedrohungen und Anomalien geben. Die Nutzung solcher Daten ermöglicht die Umsetzung von Gegenmaßnahmen oder neuen Schutzmethoden, die für Sicherheitslösungen zur Verfügung stünden.

Multi-Layer Collaborative Security

by Stormshield

1 Gemeinschaftlicher Schutz

Die Schutz-Engines eines Systems wie z.B. einer multifunktionalen Firewall oder eines Arbeitsplatzschutzes, tauschen Informationen über beobachtete schwache Signale aus.



2 Kontextabhängiger Schutz

Die verschiedenen Sicherheitslösungen des Informationssystems arbeiten zusammen, um ihre schwachen Signale auszutauschen.

3 Globaler Schutz

Die Nutzung dieser Informationen würde anschließend die Implementierung von Gegenmaßnahmen oder neuen Schutzmethoden in Sicherheitslösungen ermöglichen.

GEMEINSCHAFTLICHER SCHUTZ

Die erste Schicht des neuen Ansatzes beinhaltet das Integrieren der Security Engines einer Sicherheitslösung, so dass sie später zusammenarbeiten können. Beispielsweise bieten Multifunktionsschutzlösungen und New-Generation Firewalls mehrere Sicherheitskomponenten. In der Regel enthalten diese Produkte Traffic-Filterungsfunktionen sowie Intrusion Prevention, Antivirus, Antispam, URL-Filter, Data Leak Prevention und sogar Schwachstellenerkennung.

Jedoch berücksichtigen diese Funktionen nur den Kontext, den sie auch berücksichtigen sollen. Die Netzwerk-Traffic-Kontrolle sowie Filterfunktionen sind in der Lage, verdächtigen Hosts den Zugriff zu verweigern. Intrusion Prevention kann einen Alarm auslösen, wenn ein Arbeitszugriff im Netzwerk verdächtig erscheint oder ein neuer Command-and-Control-Kanal auftaucht. Das Antispam-Modul meldet Informationen zu den wichtigsten Empfängern unerwünschter E-Mails, die zu sozialen Netzwerken verlinken. Zudem kann die Schwachstellenerkennung die Risikostufe für die angeschlossenen Rechner im Unternehmen abbilden.

Auch wenn jede Komponente unabhängig voneinander läuft, was auch die Grenzen des Silo-Schutzes widerspiegelt, können die einzelnen Engines zusammenarbeiten, um das Sicherheitsniveau zu erhöhen. Bei der Verarbeitung von Traffic oder Daten würde jedes Modul die durchgeführten Vorgänge sowie die von anderen Modulen bereitgestellten Informationen berücksichtigen. Bei der Beurteilung des Verhaltens würde das Sicherheitsmodul gemäß dem Kontext des wahrscheinlichen Angriffs handeln.

Beim Beispiel eines gefährdeten Hosts, der zum Besuch einer kategorisierten Webseite verwendet wird, besteht keine besondere Gefahr – und die Webseite stellt nur ein mäßiges Risiko dar. Wenn das URL-Filter-Modul allerdings von dem Seitenbesuch des gefährdeten Hosts weiß und interaktive Verbindungen nachgewiesen wurden, kann der Zugang zu dieser Webseite blockiert werden.

Auf diese Weise würde jedes Sicherheitsmodul etwas zum Gesamtschutz auf der Ebene der New Generation Firewalls beitragen. Anstatt einen Vorfall mit geringem Risiko einfach zu erlauben, kann ein bestimmtes Modul ein schwaches Signal aufzeichnen und so die damit verbundene Risikostufe präzise feststellen.

Wenn ein anderes Modul anschließend einen Vorfall auf dessen Bezug zum vorherigen Ereignis analysiert, könnte das Modul die Risikostufe erhöhen oder den Zugang blockieren. Die verschiedenen Risikostufen hätten ihre eigene Gewichtung, die dann von den Schutzmodulen beim Erkennen von Attacken herangezogen werden könnte. Jedes Modul würde die verarbeiteten Ereignisse samt Risikograd (definiert durch ein anderes Modul) korrelieren, um Bedrohungen so ganzheitlich betrachten und prüfen zu können.

Das Schutzsystem könnte nach der ganzheitlichen Analyse eine gezielte Aktion auslösen, z.B. Traffic blockieren oder einen verdächtigen Host in der Sanierungszone

unter Quarantäne stellen. Die Bedrohung würde dann blockiert oder abgeschwächt, wodurch sich das allgemeine Schutzniveau erhöhen würde.

KONTEXTABHÄNGIGER SCHUTZ

Die zweite Schicht dieses neuen Ansatzes ist umfassender, weil ein Unternehmen schließlich Schutzsysteme an mehreren Standorten innerhalb der Infrastruktur einsetzt. Eine New Generation Firewall sichert Netzwerkzugriffe sowie den Datenverkehr im Unternehmensnetzwerk ab. Ein auf den Arbeitsplatzrechnern eingesetztes System fängt zudem die anspruchsvollsten Zero-Day-Bedrohungen ab und untersucht andere Angriffsvektoren (USB-Stick, Fahrlässigkeit oder internen Missbrauch).

Nach dem gleichen Prinzip der Korrelation von schwachen Signalen wird die Zusammenarbeit zwischen diversen Sicherheitslösungen ermöglichen, das Schutzniveau nochmals zu erhöhen. Dabei berücksichtigt man nicht nur Ereignisse, die im Zusammenhang mit bestimmtem Netzwerkverkehr oder einem Workstation-Schutz stehen, sondern alle verfügbaren Informationen innerhalb des Konzerns. Der Schutz wäre somit kontextabhängig.

Gehen wir zurück zu unserem Beispiel des gefährdeten Hosts: Hier liefert der Mechanismus der Schwachstellenerkennung noch genauere Kontextinformationen. In der Tat würde eine Analyse der Schwachstellen ein potenzielles Risiko im Zusammenhang mit einer unsicheren Applikation offenbaren – egal, ob sie bereits befallen und ausgenutzt wird oder nicht. Hat die New Generation Firewall ein solches Verhalten erfasst, kann die Schutzlösung der Workstation illegale Speicherzugriffe oder die verbotene Nutzung eines USB-Sticks aufdecken. Solche Informationen würden die Einschätzung der Risikostufe noch präziser machen.

Sicherheitssysteme müssen ihre Zusammenarbeit noch stark verbessern und mehr Informationen austauschen, um das Schutzniveau zu erhöhen. Die New Generation Firewall könnte den Netzwerkzugriff dann einschränken und Hosts, auf deren Speicher illegal zugegriffen wurde, in eine Quarantänezone verweisen. Das Schutzsystem eines Arbeitsplatzrechners könnte darüber hinaus die Sicherheitsrichtlinien ändern, z.B. indem Hosts isoliert oder deren Zugriff ausschließlich auf von Bedrohungen befreite Server beschränkt wird. Ebenso wäre es möglich, dass Workstation-Systeme Informationen über illegale Inhalte mit der Firewall teilen, um Ungleichmäßigkeiten zusammenzufassen, die durch Angriffe verursacht wurden, oder um Hosts ohne erweiterte Schutzsysteme abzusichern.

GLOBALER SCHUTZ

Da Cyberkriminelle weltweit zuschlagen, wäre dementsprechend eine global angelegte Reaktion die am besten geeignete. Schutzlösungen auf der ganzen Welt richten sich nach den neuesten Angriffstechniken, die global auftreten, und bieten sowohl aktive als auch proaktive Reaktionen.

Dieser Ansatz wird bereits seit vielen Jahren von Antivirus-Software-Herstellern umgesetzt. Sobald die gesammelten Daten analysiert wurden, werden Berichte zu aktuellem Angriffsverhalten sowie den zuletzt verwendeten Vektoren erstellt. So ist es möglich, Schutzmechanismen zu verbessern und selbst auf Zero-Day-Attacken adäquat zu reagieren. Die weltweite Datensammlung ermöglicht eine umfassende Reaktion auf die Bedrohung.

Neben den neuen Exploits könnten auch konsolidierte Daten analysiert werden, um zu verstehen, wie Vektoren und Viren aufeinander abgestimmt sind. Auf diese Weise wäre man in der Lage, neue Angriffstechniken zu antizipieren. Durch das Einbeziehen internationaler Organisationen wie CERT, SOCs oder MSSPs kann die Datensammelzone zusätzlich ausgeweitet werden. Dazu gehören Schutzlösungen unterschiedlicher Herkunft und aus verschiedenen Operation Centers, die die Sicherheit überwachen, um eine noch breiter angelegte Reaktion auf Angriffe geben zu können. Zusätzlich zum zuvor erwähnten quantitativen Aspekt sollten die Organisationen auch in der Lage sein, einen qualitativen Ansatz für neue Verhaltensweisen zu liefern.

Der kollaborierende Austausch von Online-Bedrohungsdaten mit einem Sicherheitsökosystem hilft darüber hinaus bei der Planung wirksamer Gegenmaßnahmen. Dabei gibt es drei mögliche Arten von Reaktionen:

- Eine Signaturdefinition macht es möglich, auf eine entdeckte Attacke zu reagieren. Allgemein kann die Signatur der genutzten Virusbelastung identifiziert werden.
- Die Verhaltensreaktion bietet Schutz auf Basis der berechtigten Nutzung einer Ressource (Netzwerk, Speicher oder Datenregister). Das Ausnutzen einer Zero-Day-Schwachstelle wird dadurch antizipiert.
- Die kontextabhängige Antwort berücksichtigt alle Schutzmodule. Dieser Ansatz kann die Gewichtung verschiedener schwacher Signale ändern – entsprechend den Daten, die kürzlich gesammelt wurden.

Diese Gegenmaßnahmen könnten in Form von neuen Signaturen, Software-Upgrades oder Konfigurationsempfehlungen eingesetzt werden. Damit würde die Informationssicherheit auf globaler Ebene gestärkt.

Stormshields Ansatz

Als Reaktion auf die Gefährdung kritischer Services und abgesaugte sensible Unternehmensdaten bietet **Stormshield eine Bedrohungsüberwachung auf globaler Ebene sowie ein umfassendes System zum koordinierten Schutz an.**

Der neue **Multilayer Collaborative Security-Ansatz** ist Stormshields Basis, um die Sicherheit zu verbessern. Zugleich ist der Ansatz der Kern der Entwicklung der Multifunktionslösungen und des Multiproduktportfolios

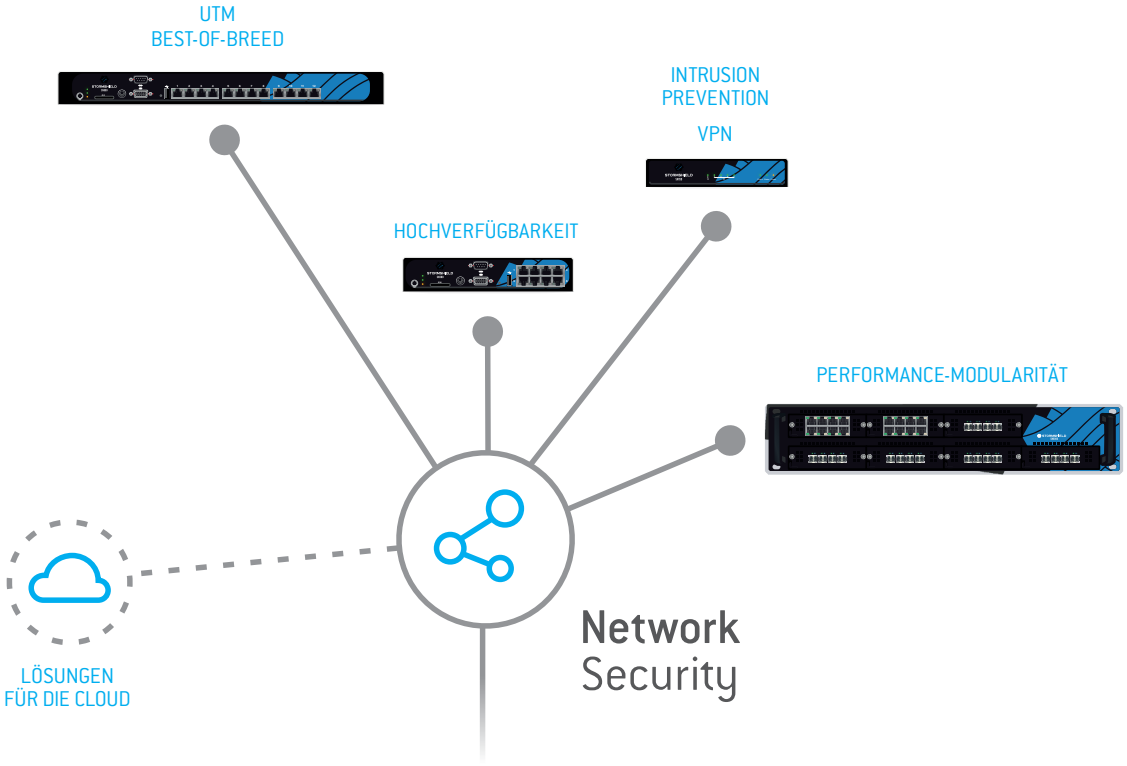
Die **Stormshield Network Security**-Produktspanne setzt sich aus einer Reihe von Multifunktionsnetzwerkschutzlösungen zusammen, die neben weiteren Eigenschaften ein Schwachstellenmanagementmodul integriert haben.

Stormshield Endpoint Security-Produkte bieten einen wirksamen Workstation-Schutz, der auf die anspruchsvollsten Angriffe reagieren kann. **Stormshield Data Security** schützt empfindliche Informationen und garantiert eine wirksame Barriere gegenüber Datenlecks*.

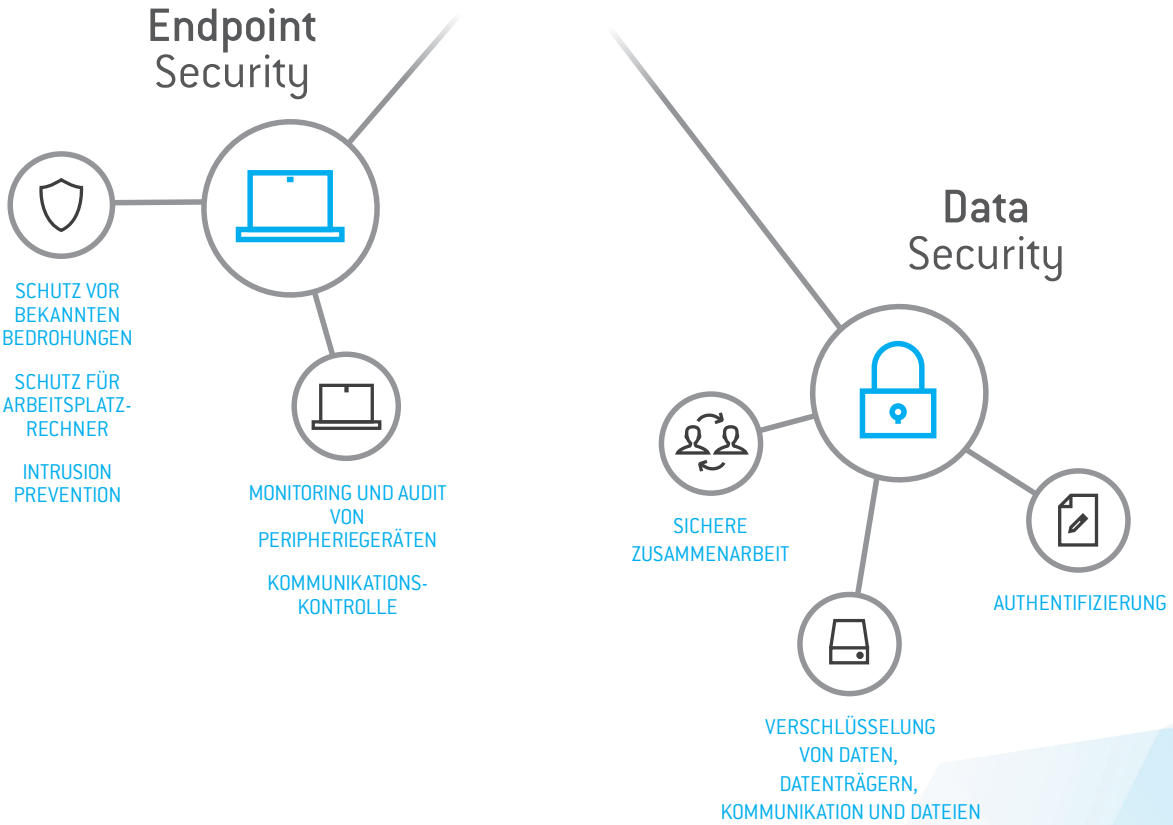
Durch die Zusammenarbeit der Sicherheitsmodule und -produkte ist Stormshield in der Lage, eine Antwort auf die ersten beiden Schichten des kollaborierenden Ansatzes zu geben. Die Art und Weise der Informationen, die die eingesetzten Produkte mitteilen, stellt sicher, dass alle Kunden eine globale Sicht auf die Bedrohung erhalten*.

Diese Synergie unterstützt die Vision von Stormshield. Diese besteht aus der Reaktion auf Multivektor-Bedrohungen durch effektiven und mehrschichtigen Schutz, interne Zusammenarbeit, kontextabhängigen Schutz und eine globale Analyse von Bedrohungen.

* kann deaktiviert werden



MULTI-LAYER COLLABORATIVE SECURITY



STORMSHIELD

Telefon
+49 (0) 89 57959 404

WWW.STORMSHIELD.EU

Regus Offices
Landsberger Strasse 155, 80687 München
DEUTSCHLAND