WHITEPAPER ADVANCED ENDPOINT SECURITY

v.1.0

Carsten Dibbern, 20.10.2015

1. CLIENTS IM FOKUS DER ANGRIFFE

Die IT-Sicherheitslage in Unternehmen hat sich in den letzten zwei Jahren massiv geändert. Waren bisher die Angriffsszenarien eher theoretischer Natur, werden heute zahlreiche Unternehmen regelmäßig erfolgreich angegriffen. Diese Angriffe sind erfolgreich, obwohl zahlreiche Sicherheitsmaßnahmen getroffen und verschiedenste Sicherheitsmaßnahmen im Einsatz sind. Dies liegt in erster Linie daran, dass die Angriffe zielgerichtet erfolgen. Sicherheitsmaßnahmen, die auf bekannte Angriffe reagieren, wie Virenschutz-Lösungen mit Signaturerkennung, greifen nicht.

Damit ist das Mittel wirkungslos, worauf sich viele in der Vergangenheit verlassen haben. In jeder Sicherheitspolicy wird der Umgang mit Virenschutz beschrieben und auf den unterschiedlichsten Systemen als Pflichtmaßnahme gefordert. Das geht sogar so weit, dass diese Policys auf mobile Endgeräte angewendet werden, für die ein Virenschutz wenig Sinn hat.

Angreifer müssen sich heute nicht die Mühe machen, moderne mobile Endgeräte anzugreifen. In der Regel haben diese sowieso nur begrenzt Zugriff in die Unternehmen. Viel einfacher ist es, normale Clients – Desktops oder Notebooks – auf eine infizierte Webseite zu leiten oder eine E-Mail mit einem infizierten Anhang zu verschicken.

Es werden in erster Linie bekannte Schwachstellen derjenigen Anwendungen ausgenutzt, die ein Nutzer am häufigsten nutzt: Browser mit ActiveX, Flash und Java, Adobe Reader und Microsoft Office. Das heißt, allein mit einem guten Patchmanagement könnten viele Angriffe verhindert werden. Browser, Java und Flash sind aber nicht ohne Grund häufig nicht mit den neuesten Patchen versehen. Sehr häufig werden im Intranet Anwendungen eingesetzt, die nicht mit den neuesten Programmversionen der Browser oder Java funktionieren, sodass nicht zeitnah gepatcht werden kann.

Aber auch ein optimal gepatchter Client birgt Risiken. Es gibt einen schwunghaften Handel von nicht veröffentlichten Schwachstellen, für die es keine Patche gibt. Gegen diese Angriffe sind Clients mit einer klassischen Clientsicherheitsmaßnahme schutzlos. Auch die Sicherheitsmaßnahmen im Unternehmensnetz – Firewalls, IPS, E-Mail-und Web-Sicherheitsgateways – bieten hier keinen Schutz. Noch schlimmer, ein Angriff wird noch nicht einmal bemerkt.

Es werden also Maßnahmen benötigt, die sowohl einen nicht perfekt gepatchten Client als auch vor fortgeschrittenen Angriffen mit 0-Day-Exploits schützen. Computacenter hat dazu die aktuellen Produkte evaluiert und in einem Portfolio zu Advanced Endpoint Security zusammengestellt.

2. CLIENT-SICHERHEITSSTRATEGIE

Um Unternehmens-Clients gegen zielgerichtete Angriffe abzusichern, ist es erforderlich, die Schutzziele zu schärfen. Keine Sicherheitsmaßnahme schützt zu 100 %, jede ist umgehbar. Es ist eine Frage der benötigten Mittel und des Aufwands.

Es muss individuell definiert werden, vor welchen Angreifern man sich schützen möchte, und mit welcher Intensität man Widerstand leisten möchte. Dazu zieht man die Bewertung einer potenziellen Schadenshöhe eines Angriffs und die Wertigkeit potenziell gestohlener Daten heran. Kein Angreifer wird mehr in einen Angriff investieren, als er potenziell an Gewinn erzielen kann.

Zusätzlich ist relevant, wie die Clients in ein Unternehmen integriert sind. In einer Architektur, in der Clients lose an das Unternehmen gekoppelt sind, erfolgen Zugriffe auf kritische Ressourcen mit separaten Authentisierungen, und die Daten verbleiben auf den zentralen Servern. Diese Architektur führt zu einer anderen Risikoeinschätzung als eine Architektur, in der Clients Bestandteil der Unternehmensinfrastruktur sind und die zahlreiche Zugriffsmöglichkeiten auf andere Systeme und Daten ermöglicht. In diesem Fall bietet ein kompromittierter Client Angreifern wesentlich mehr Möglichkeiten.

Für die Erstellung einer Sicherheitsarchitektur und Lösungsauswahl gilt es neue Paradigmen aufzustellen:

- Es muss davon ausgegangen werden, dass Clients bereits kompromittiert sind: „Assume breach". Auch dann müssen Maßnahmen existieren, die einen Angriff erkennen können und eine Ausbreitung auf andere Systeme, insbesondere auch auf die einer höheren Schutzzone, erschweren.
- Die Wirksamkeit einer Sicherheitsmaßnahme muss aus der Sicht eines Angreifers bewertet werden.
- Sicherheitsmaßnahmen müssen auch gegen zielgerichtete Angriffe eine Schutzwirkung zeigen.
- Sicherheitsmaßnahmen müssen sich kombinieren lassen: „best integrated".
- Anwenderbedürfnisse müssen berücksichtigt werden.

3. VORBEREITUNG

Um sich gegen zielgerichtete Angriffe zu wappnen, kommt man um ein paar Hausaufgaben nicht herum. Im Folgenden wird auf die vorbereitenden Maßnahmen eingegangen.

ANWENDUNGSINVENTARISIERUNG – „IST-ZUSTAND"

Um die Clients gegen zielgerichtete Angriffe schützen zu können, müssen die Clients und Anwendungen bekannt sein. Es wird daher eine Inventarliste aller Clients und aller installierten Anwendungen benötigt. Andernfalls braucht man sich mit dem Thema Advanced Endpoint Security gar nicht erst zu beschäftigen. Diese Clients werden dann in eine entsprechende Risikostufe eingeordnet, die der Stufe „Client ohne Maßnahmen gegen zielgerichtete Attacken" entspricht.

In der Praxis ist eine Anwendungsinventarisierung keine triviale Aufgabe, zumal sich auch Anwendungen mit User-Rechten installieren lassen, wie selbst heruntergeladene Browser. Es reicht also nicht nur, diejenigen Anwendungen aufzunehmen, die über die zentrale Softwareverteilung installiert wurden.

Anwendungen, die über das Netzwerk kommunizieren, kann man z. B. am Proxy identifizieren und auch sperren. Sehr hilfreich ist auch die Nutzung von zentralen Scannern, die automatisch die Anwendungen der Clients aufnehmen. Dazu können z. B. Schwachstellenscanner im sogenannten „Credential Scan"-Modus neben ihrer Aufgabe, Schwachstellen aufzunehmen, auch dazu verwendet werden, die installierten Anwendungen aufzunehmen.

ANWENDUNGSAUSWAHL – „SOLL-ZUSTAND"

Neben der Inventarliste der Anwendungen muss das „Soll" definiert werden. Dabei werden alle erlaubten Anwendungen bestimmt. Dabei muss insbesondere sichergestellt werden, dass diese aus einer sicheren Quelle stammen. Diese Auswahl wird mit der Inventarliste, dem

„Ist", abgeglichen. Bei einem Delta wird ein Prozess gestartet, der entweder das „Soll" anpasst oder dafür sorgt, dass die ungewollte Anwendung entfernt wird.

Die Bestimmung der „erlaubten" Client-Applikationen ist für viele Unternehmen eine Herausforderung. Oft sind viele hundert verschiedene Programme im Einsatz und werden auch von den Anwendern benötigt. Trotzdem sollte dieser Zustand kein Freibrief sein, dieses Thema nicht in den Griff zu bekommen. Ohne eine Kenntnis des Software-Zustands der Clients können keine speziellen Sicherheitsmaßnahmen getroffen werden. Spätestens beim Thema Lizenzmanagement und Betriebssystemmigration ist ein Applikationsmanagement ebenfalls Voraussetzung.

GRUPPIERUNG VON CLIENTS

Für eine geeignete Auswahl von Schutzmaßnahmen und eine Schutzbedarfsfeststellung werden Clients in Typen und Gruppen sortiert, z. B. Clients von Administratoren, Clients in Entwicklungsabteilungen oder im Servicedesk, mobile Clients mit Remote-Zugängen ins Unternehmen, mobile Clients mit direktem Zugang ins Internet usw.

REVIEW DER SECURITY-INCIDENT-RESPONSE-PROZESSE

Nahezu in jedem Unternehmen sind bereits Sicherheitsprodukte im Einsatz. Besonders lohnenswert ist eine Untersuchung des Betriebs der im Einsatz befindlichen Virenschutzlösung. Auch wenn diese nur begrenzt Schadcode erkennt, so ist häufig der Prozess des Viren-Incident-Handlings nicht optimal und zufriedenstellend. Bevor hier nicht saubere Prozesse und Zuständigkeiten definiert sind, ist der Einsatz von Technologien, die fortgeschrittene Angriffe melden, nicht sinnvoll.

4. LÖSUNGSARCHITEKTUR – ENDPOINT SECURITY

Im Folgenden werden verschiedene Komponenten aufgeführt. Dabei wird die Effektivität des Schutzes nach präventiver, detektiver und reaktiver Wirkung getrennt tabellarisch aufgeführt.

4.1 ARCHITEKTUR BISHER

Im Folgenden ist eine klassische Sicherheitsarchitektur aufgeführt, wie sie häufig aufzufinden ist.

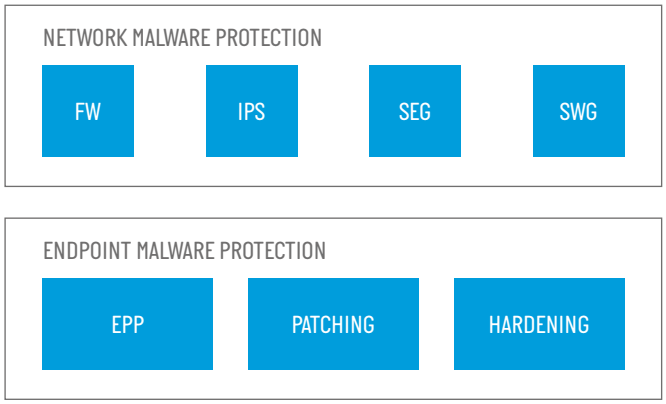

Abbildung 1: Klassische Architektur für Endpoint Security

Es werden Komponenten im Netzwerk und Komponenten auf dem Client eingesetzt:
Die Firewall (FW) begrenzt die Kommunikation mit dem Internet auf ausgehendes http und https. Das IPS untersucht den unverschlüsselten Netzverkehr vom Internet nach Angriffsversuchen auf bekannte Schwachstellen. Das Sicherheits-Web-Gateway (SWG) begrenzt als Proxy mit URL-Filtern den Web-Verkehr auf erlaubte Zieladressen und prüft mit einem Virenscanner heruntergeladene Dateien auf bekannte Malware, ggf. mit SSL-Entschlüsselung.

Das Sicherheits-E-Mail-Gateway (SEG) prüft E-Mails auf Spam und bekannte Malware.

Am Endpunkt wird eine Endpoint-Protection-Plattform (EPP) eingesetzt, die bekannte Malware erkennen und entfernen kann. In der Regel werden lediglich Betriebssystem-Patche zeitnah verteilt. Client-Hardening wird in einer Basisvariante eingesetzt, allerdings verfügen Nutzer sogar oft über lokale Administrationsrechte am Client.

WIRKUNG GEGEN	PRÄVENTION	DETEKTION	REAKTION
bekannte Angriffe	+	+	+
gezielte Angriffe auf bekannte Schwachstellen	-	o	+
gezielte Angriffe mit 0-Day-Schwachstellen	-	-	-
bereits installierten Schadcode	o	o	-

++ stark , + gut, o eingeschränkt, - nicht vorhanden

Tabelle 1: Klassischer Schutz von Endgeräten – qualitative Darstellung

Bekannter Schadcode kann vom Virenschutz oder vom IPS erkannt, geblockt und entfernt werden. Gezielte Angriffe auf bekannte Schwachstellen können noch teilweise vom IPS erkannt werden. Schadcode, der sich bereits im Unternehmen befindet, wird erst dann entdeckt, wenn er sich auffällig verhält, z. B. indem er sehr große Datenmengen bewegt oder die Leistung eines Clients stark einschränkt.

Die meist verbreitete Sicherheitsarchitektur schützt nicht gegen zielgerichtete Angriffe.

4.2 KOMPONENTEN AUS DEM ADVANCED-ENDPOINT-SECURITY-PORTFOLIO

Im Folgenden werden einzelne Komponenten aufgeführt und ihre Wirkung gegen bekannte Angriffe, gegen gezielte Angriffe unter Ausnutzung bekannter Schwachstellen und gegen Angriffe unter Ausnutzung von 0-Day-Schwachstellen aufgeführt.

Keine präventive Sicherheitslösung wirkt zu 100 %. Mit dem Paradigma „assume breach" werden Mittel benötigt, um Attacken im Unternehmen zu entdecken und schnell zu bekämpfen. Daher gehören zu einer modernen Sicherheitsarchitektur neben präventiven Maßnahmen auch Komponenten mit detektiver und reaktiver Wirkung.

Präventive Wirkung meint: Ein Schadcode wird in der Phase der Zulieferung zum Client, bei der Ausnutzung einer Schwachstelle oder bei der Installation gehindert. In jedem Fall wird verhindert, dass der Angreifer sein Angriffsziel erreicht.

Maßnahmen mit detektiver Wirkung enthalten Funktionen, die einen Schadcode anhand bestimmter Eigenschaften entdecken oder anhand seines Verhaltens, nachdem er sich festgesetzt hat.

Ist ein Schadcode entdeckt, werden IOCs[1] definiert, mit denen Schutzkomponenten konfiguriert werden können, sodass eine weitere Verbreitung eingedämmt wird. Dies sind Maßnahmen mit reaktiver Wirkung. Zusätzlich gehören Maßnahmen zur Client-Wiederherstellung zu den reaktiven Maßnahmen.

4.2.1 EXPLOIT MITIGATION

Die Methoden, mit der Angreifer Exploits programmieren, um Schwachstellen auszunutzen, lassen sich bestimmten Kategorien zuordnen. Letztlich zielen diese darauf ab, Speicherbereiche zu überschreiben und Code des Angreifers zur Ausführung zu bringen. Exploit Mitigation (EM) erschwert dieses, sodass einfache Exploit-Techniken nicht genutzt werden können.

Microsoft stellt das Tool EMET zur Verfügung, das kostenfrei eingesetzt werden kann. Andere Exploit-Mitigation-Produkte, wie TRAPS von Palo Alto, bieten noch erweiterte Funktionalitäten, die ein Umgehen der Sicherheitsmechanismen weiter erschweren.

Da sich Exploit Mitigation auf die Exploit-Techniken selbst stützt, ist es auch wirksam gegen 0-Day-Angriffe. EM-Tools ist Software auf dem Client, die als Kernelmodul Anwendungen beim Start über Prozess-Hooks erweitern. Da sie auf den Anwendungscode selbst keinen Einfluss nehmen, haben sie minimale Performanceauswirkungen. Da manche Anwendungen nicht konform zu den Entwicklungsrichtlinien von Microsoft programmiert oder kompiliert wurden, kann es zu Programmabstürzen kommen. Daher muss jede Anwendung, die in EM integriert wird, einen Testzyklus durchlaufen. Für weit verbreitete Standardanwendungen sind diese Tests bereits vom EM-Toolhersteller durchgeführt.

WIRKUNG GEGEN	PRÄVENTION	DETEKTION	REAKTION
bekannte Angriffe	+	+	-
gezielte Angriffe auf bekannte Schwachstellen	+	+	-
gezielte Angriffe mit 0-Day-Schwachstellen	+	+	-
bereits installierten Schadcode	-	-	-

++ stark , + gut, o eingeschränkt, - nicht vorhanden
Tabelle 2: Exploit Mitigation

4.2.2 APPLICATION CONTAINMENT

Eine Application-Containment-Lösung sorgt dafür, dass eine Applikation in einem isolierten Kontext läuft. Auch wenn ein Exploit eine Schwachstelle einer Applikation ausnutzt, so sorgt die Isolation dafür, dass sich der Schadcode nur in dem isolierten Kontext einpflanzen kann. Damit kann sehr wirkungsvoll verhindert werden, dass ein Schadcode Wirkung zeigt. Application Containment wirkt nur auf die Anwendungen, die in dem Containment laufen. Es wird für diejenigen Anwendungen eingesetzt, die den höchsten Risiken ausgesetzt werden – in erster Linie Browser und Anwendungen, die Daten aus dem Internet verarbeiten, wie Textverarbeitung, Office und Adobe Reader.

Application Containment bietet keinen Schutz, wenn ein Nutzer eine Anwendung nutzt, die er selbst installiert hat. Es ist also wichtig, hier mindestens eine Applikationsinventarisierung einzusetzen oder eine Application-Control-Lösung.

Es gibt verschiedene Techniken, Containment umzusetzen:

- Remote-Controlled Browsers Systems (RECOBS): Diese Methode ist im strengeren Sinne kein Application Containment, da sie nicht an einer Applikation selbst wirkt. Den Clients wird der direkte Zugang zum Internet komplett verweigert. Stattdessen wird ein Zugang zum Internet über Terminalserver bereitgestellt. Das BSI hat hierfür ein eigenes Schutzprofil[2], nach dem sich Anbieter zertifizieren lassen können. In Behörden und Banken findet dieser Ansatz die meiste Verbreitung. Der sehr hohen Schutzwirkung stehen einige funktionale Einschränkungen entgegen, z. B. eingeschränktes Video-Streaming und eingeschränkte Geschwindigkeit. Zudem ist diese Methode für Notebooks nur einsetzbar, wenn alle Netzverbindungen des Notebooks über das Unternehmens-VPN erzwungen werden.
- Browser-Virtualisierung: Der Browser wird in einem separaten gehärteten Betriebssystem, das in einem Hypervisor läuft, genutzt (z. B. BitBox von Sirrix[3]). Im geschäftlichen Umfeld wird diese Methode bisher kaum genutzt. Grund ist die hohe Ressourcenverwendung und lange Startdauer des Browsers, da ein komplettes Betriebssystem virtualisiert wird. Eine weitere Herausforderung ist, dass man mit Zusatzkomponenten dafür sorgen muss, dass nur der BitBox-Browser Zugang zum Internet erhält.
- Sandbox: Die Applikation wird unter einem eigenen eingeschränkten System-User gestartet. Dabei werden die Standardmittel des Betriebssystems genutzt. Mit dieser Methode können neben dem Browser auch andere Anwendungen isoliert werden. Da Basis-Betriebssystemfunktionen genutzt werden, werden kaum zusätzliche Systemressourcen benötigt, und es besteht eine hohe Kompatibilität. Beachtet werden muss, dass aufgrund der Nutzung von Betriebssystemfunktionen diese Methode nicht vor Kernel-Exploits schützt. Eine Verbindung mit Application Control ist hier sinnvoll. DefendPoint von Avecto nutzt z. B. diesen Ansatz.
- Mikro-Applikationsvirtualisierung: Die Applikation greift nicht direkt auf das Betriebssystem des Clients zu, sondern über die Hardware-Virtualisierung des Prozessors[4].
  Kernfeatures:
  – Strenge Umsetzung der Sicherheitsprinzipen: Default deny, least privileged

[1] Indicator of compromise: Begriff aus der Computerforensik. Nachdem ein Schadcode identifiziert wurde, wird definiert, woran er zu erkennen ist, z. B. anhand einer bestimmten Quelle, Nutzung bestimmter Krypto-Bibliotheken oder eine bestimmten Signatur.
[2] https://www.bsi.bund.de/SharedDocs/Zertifikate/PP/aktuell/PP_0040.html
[3] Im Auftrag des BSI entwickelt und für Privatnutzer kostenfrei, http://www.sirrix.de/content/pages/BitBox.htm
[4] Intel Core i3, i5, i7 mit Intel® Virtualization Technology (Intel® VT) oder AMD Processor mit Rapid Virtualization Indexing

- Betriebssystem-Funktionen werden ausschließlich nach „need to know" bereitgestellt, d. h. Registry, Datei-System, USB, Kamera, Speaker etc., nur wenn erforderlich
- „Copy on Write", d. h., der Prozess der Applikation schreibt nicht in den echten Speicher des Gerätes, sondern nur in ein virtuelles Abbild des Speichers.

In dieser Variante bemerkt der Nutzer so gut wie nicht, dass seine Anwendung virtualisiert ist. Für Browser werden alle Funktionen wie Video-Streaming, Kamera oder Mikrofon unterstützt. Hersteller dieser Produkte sind sehr bemüht, die unterstützten Anwendungen ständig zu erweitern. Gängige unterstützte Anwendungen sind Browser mit Add-ons (Flash, Java, Silver-Light), Office, Outlook, Media Player. Der Hersteller Bromium ist hier einer der führenden Anbieter.

WIRKUNG GEGEN*	PRÄVENTION	DETEKTION	REAKTION
bekannte Angriffe	++	+	-
gezielte Angriffe auf bekannte Schwach-stellen	++	+	-
gezielte Angriffe mit 0-Day-Schwachstellen	++	+	-
bereits installierten Schadcode	-	-	-

++ stark , + gut, o eingeschränkt, - nicht vorhanden
*bezieht sich auf Mikrovirtualisierung
Tabelle 3: Application Containment

Application Containment bietet für Browser eine sehr gute Schutzwirkung. Es kann sinnvoll sein, das weitere Gesamtkonzept zur Erkennung von Browser-Schadcode anzupassen, z. B. könnte man Content-Filterung am Web-Proxy und netzwerkbasiertes Sandboxing von HTTP-Verkehr nur für diejenigen Clients einsetzen, deren Browser nicht durch Application Containment geschützt ist bzw. als Notnagel verwenden, falls Application Containment aus Versehen deaktiviert ist.

Auch kann es ein wichtiges Argument sein, für Notebooks direktes Surfen im Internet zuzulassen.

4.2.3 APPLICATION CONTROL UND PRIVILEGE MANAGEMENT

Werden die Anwendungen auf einem Client so kontrolliert, dass nur bekannte Prozesse laufen können, wird verhindert, dass installierter Schadcode zur Ausführung kommt. Gleichzeitig werden vom Nutzer installierte Anwendungen kontrolliert und gegebenenfalls an der Ausführung gehindert.

Bisher wurde Application Control im Wesentlichen auf Systemen eingesetzt, die wenig Dynamik ausgesetzt waren, wie Rechner in Industrieanlagen oder Geldautomaten. Seit Windows 7 mit AppLocker ist auch Application Control für Clients im Fokus. Mit verschiedenen Regelsätzen lässt sich Application Whitelisting konfigurieren. Für mehr Flexibilität mit diversen Workflowunterstützungen und Selfservices für Ausnahmeprozesse gibt es Zusatztools, die auch einen Einsatz von Whitelisting in komplexen Client-Umgebungen ermöglichen. Voraussetzung ist wieder die in Kapitel 3 genannte Anwendungsinventarisierung.
Die Einschränkung der Nutzerrechte auf einem Client ist eines der Grundprinzipien für Client-Sicherheit. Zum einen wird so verhindert, dass der Nutzer in Unwissenheit problematische Software nachinstalliert, zum anderen erschwert es, dass ein Schadcode privilegierte Rechte erreicht.

Unternehmen, denen eine starre Wegnahme von Administrationsrechten bisher nicht möglich war, können dedizierte Client-Privilege-Management-Lösungen einsetzen. Diese bieten u. a. die Möglichkeit, Prozesse zur temporären Rechteerweiterung am Client zu etablieren, z. B. um Änderungen an der Netzwerkkonfiguration vorzunehmen. Des Weiteren ermöglichen sie es auch, Anwendungen, die lokale Administrationsrechte benötigen, damit auszustatten, ohne dass der Nutzer diese bekommt.

Avecto DefendPoint bietet genau diese Kombination aus Anwendungs- und Rechtekontrolle.

WIRKUNG GEGEN	PRÄVENTION	DETEKTION	REAKTION
bekannte Angriffe	+	o	-
gezielte Angriffe auf bekannte Schwach-stellen	+	o	-
gezielte Angriffe mit 0-Day-Schwachstellen	+	o	-
bereits installierten Schadcode	+	-	-

++ stark , + gut, o eingeschränkt, - nicht vorhanden
Tabelle 4: Privilege Management und Application Control

Durch die Kombination aus Einschränkung der Nutzerrechte und Applikationskontrolle erhöht sich die Widerstandsfähigkeit gegen zielgerichtete Angriffe deutlich. Allein Angriffe, die durch Exploits von erlaubten Programmen direkt in den Systemkontext gelangen und die Ausführungsverhinderung von unbekannten Prozessen umgehen, kommen noch zum Zuge.

4.2.4 NETWORK BASED MALWARE PROTECTION SYSTEM

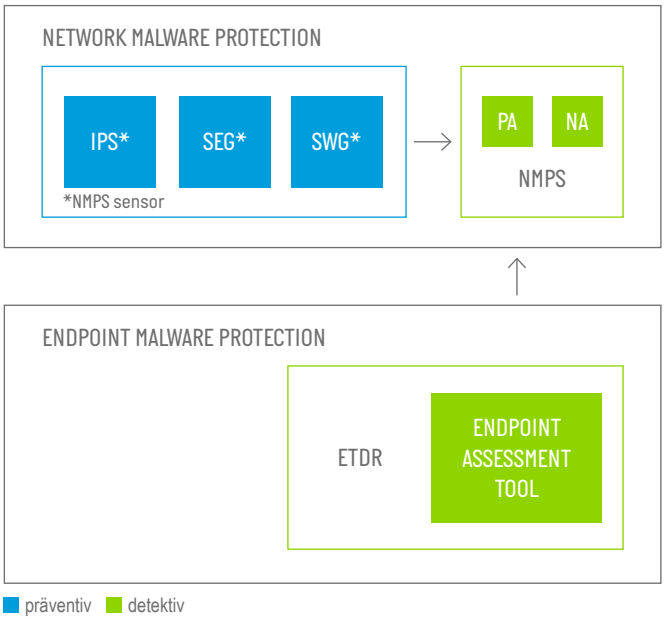

Abbildung 2: Network based malware Protection Systems

Für die Erkennung von zielgerichteten Angriffen, die über das Unternehmensnetzwerk eindringen, sind netzwerkbasierte Malware-Protection-Systeme (NMPS) gut geeignet.

Die Payload-Analyse-Komponente (PA) eines NMPS konzentriert sich auf die Untersuchung der „Payload" eines Angriffs. Dieses greift im Netzwerk die Client-Kommunikation ab und prüft gezielt Inhalte mit unbekanntem Vertrauensstatus. Dazu werden unter anderem Sandbox-Server, auf denen die unbekannten Inhalte in virtuellen Clients ausgeführt werden, genutzt. Diese sind als zentrale Systeme schnell implementierbar und untersuchen in erster Linie Dateien, die per Web oder E-Mail auf den Client gelangen.

Als Sandbox wird ein virtueller Client genutzt, der möglichst ähnlich dem Unternehmens-Client konfiguriert wird. Durch genaue Beobachtung des Clients nach Ausführung einer Datei wird festgestellt, ob ein ungewöhnliches Verhalten vorliegt. Dies wird durch dynamische und statische Code-Analyse ergänzt. Allerdings prüft mittlerweile moderner Schadcode, ob er in einer Sandbox ausgeführt wird, sodass eine gute Verschleierungstechnik des NMPS wichtig ist.

Die Netzwerkanalyse-Komponenten (NA) eines NMPS wirken auch in einer späteren Phase der Kill-Chain (siehe 5.2). Damit setzt die Sicherheitsarchitektur auch die Vorgabe des „Assume breach" um. Einfache Netzwerkanalysen untersuchen den ausgehenden Verkehr zum Internet auf potenzielle Kommunikation mit einem Command & Control Center oder auf ungewöhnlich hohe Datenvorkommen. Erweiterte Analysetools untersuchen auch den Verkehr zwischen Clients und zwischen Clients und Server auf ungewöhnliches Verhalten. Dabei werden statistische Methoden und „machine learning" eingesetzt, um normales von unnormalem Verhalten zu unterscheiden.

Mit einem Endpoint-Assessment-Tool können bei einem Event Indizien von den Clients gezogen werden, um z. B. zu erkennen, auf welchem Client eine schadhafte Datei tatsächlich ausgeführt wurde. Zusätzlich werden sie genutzt, um ein Containment des Clients zu erwirken, um eine Ausbreitung des Schadcodes zu unterbinden. In Verbindung mit einem NMPS werden in der Regel Endpoint-Assessment-Tools vom gleichen Hersteller verwendet, da so eine optimale Interoperabilität gewährleistet ist. Endpoint-Assessment-Tools sind eine Untergruppe der nächsten Kategorie: ETDR.

WIRKUNG GEGEN	PRÄVENTION	DETEKTION	REAKTION
bekannte Angriffe	o	+	+
gezielte Angriffe auf bekannte Schwachstellen	o	+	+
gezielte Angriffe mit 0-Day-Schwachstellen	o	+	+
bereits installierten Schadcode	–	–	–

++ stark , + gut, o eingeschränkt, - nicht vorhanden
Tabelle 5: MPS – nur Payload-Analyse mit Endpoint-Assessment-Tool

WIRKUNG GEGEN	PRÄVENTION	DETEKTION	REAKTION
bekannte Angriffe	o	+	+
gezielte Angriffe auf bekannte Schwachstellen	o	+	+
gezielte Angriffe mit 0-Day-Schwachstellen	o	+	+
bereits installierten Schadcode	o	+	+

++ stark , + gut, o eingeschränkt, - nicht vorhanden
Tabelle 6: MPS – mit Payload- und Netzwerkanalyse und mit Endpoint-Assessment-Tool

4.2.5 ENDPOINT THREAT DETECTION AND RESPONSE – ETDR

Um die Aufgabe der Detektion von Schadcode am Client zu unterstützen, hat sich die Produktkategorie der ETDR-Tools entwickelt. Sie bündeln verschiedene Funktionen in unterschiedlicher Ausprägung. Sie sind in der Regel als Kernel-Modul entwickelt und so unsichtbar für Applikationen.

Diese Funktionen gehören in die Kategorie ETDR:

- Verhaltensanalyse auf Systemkernel- und Speicherzugriffsebene
- NMPS Endpoint Assessment zur Übermittlung von Informationen über Systemaufrufe, Dateizugriffe und Netzwerkkommunikation
- Endpoint-Forensik-Funktionen helfen einem Forensiker, einen Angriff nachzuvollziehen, z. B. indem Speicherabbilder zentral ausgewertet werden können. Ist ein Angriff analysiert, werden sogenannte IOCs (Indicators of Compromise) erstellt. Mit diesen IOCs kann eine Neuinfektion verhindert und Clients ermittelt werden, die ebenfalls infiziert sind.
- Endpoint Containment, um einen Client zu isolieren
- Endpoint Remediation zur Wiederherstellung eines Clients

Die detektiven und reaktiven Maßnahmen erfordern Personal, das mit diesen Informationen umgehen kann. Als Organisationeinheiten sind Cyber Defense Center geeignet, die in einem Kommadozentrum Angriffe erkennen, Reaktionen auslösen und koordinieren können. In diesem Papier wird darauf nicht vertieft eingegangen.

Der Markt des ETDR entwickelt sich zur Zeit sehr dynamisch. Es erscheint am sinnvollsten, sich auf die Komponente des Assessment-Tools zu konzentrieren, wenn ein NMPS eingesetzt wird.

WIRKUNG GEGEN	PRÄVENTION	DETEKTION	REAKTION
bekannte Angriffe	-	+	+
gezielte Angriffe auf bekannte Schwachstellen	-	+	+
gezielte Angriffe mit 0-Day-Schwachstellen	-	+	+
bereits installierten Schadcode	o	+	+

++ stark , + gut, o eingeschränkt, - nicht vorhanden
Tabelle 7: ETDR-Tool

4.3 REFERENZARCHITEKTUREN

Als Referenzarchitektur bietet sich ein Design aus einer Auswahl an präventiven, detektiven und reaktiven Maßnahmen an. Ein qualitativer Vergleich aller Maßnahmen ist im Anhang aufgeführt. Orientierung bieten die Grundsätze:

- „Defence in depths"
- „Assume breach"
- „Default deny, least privilege"

Eine spezifische Risikoanalyse, die die Einsatzszenarien der Clients berücksichtigt, priorisiert die Maßnahmen. Relevant sind u. a.:

- Risiken für den Client: Art des Internetzugangs, Nutzung des Clients, Dynamik des Anwendungs-Lifecycles
- Schutzbedarf der Daten auf dem Client
- Berechtigungen der Clientnutzer im Unternehmen

4.3.1 BEISPIEL 1: FOKUS AUF DETEKTION – RISIKEN FÜR NOTEBOOKS GESONDERT BEHANDELT

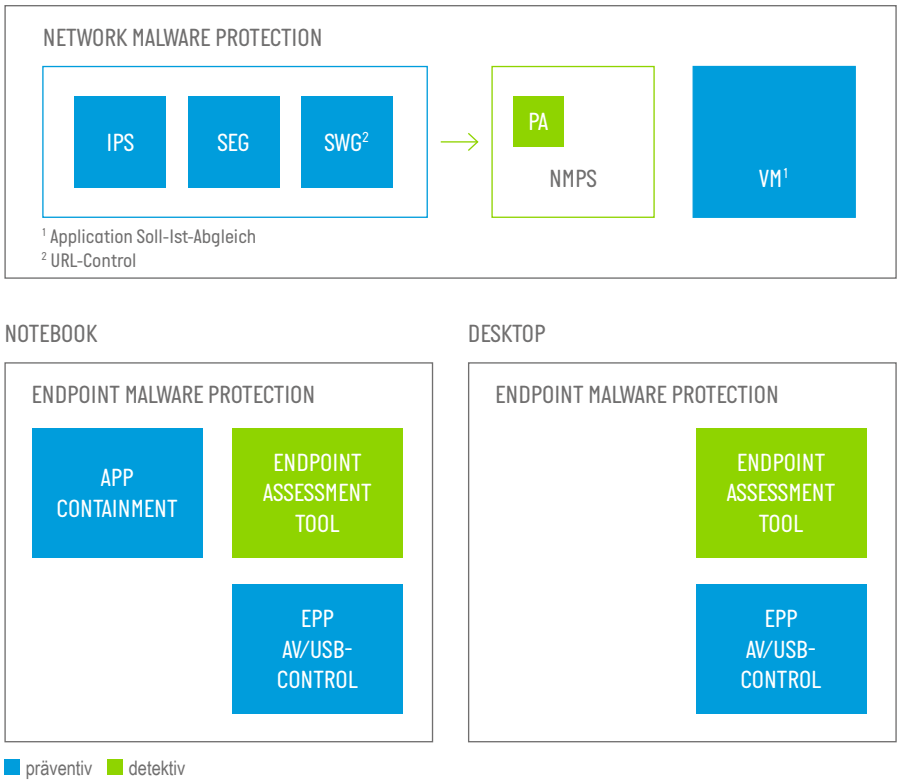

Abbildung 3: Beispiel 1 – Komponenten Advanced Endpint

++	0-Day – Prävention – Internet threats
0	Prävention – internal threats
-	Prävention – user miss behavior
++	0-Day – Detektion (payload)
+	Breach-detection
+	Reaktion
++	Geeignet für Notebook mit direktem Internetzugang
+	Kompatibilität
++	Geringe Performanceeinbußen, Ressourcenverbrauch
+	Anwenderkomfort

Abbildung 4: Beispiel 1 – Wirksamkeit

Wesentliche Architekturmerkmale:

- Zwei Client-Klassen: Notebook und Desktop
- Application Containment für besondere Absicherung von Browser und Office/Adobe für die Client-Klasse Notebooks, die direkten Zugriff ins Internet haben
- NMPS mit Payload-Analyse im Unternehmensnetzwerk zur Entdeckung von Malware im Unternehmen
- Endpoint-Assessment-Client als NMPS-Sensor für alle Clients
- Applikationsinventarisierung mit Schwachstellenscanner (VM) und zusätzlicher Prozess bei Soll-Ist-Abweichungen
- Eine klassische Endpoint Protection Suite (EPP) dient dazu, bekannte Malware mit minimalem Aufwand zu entfernen, steuert die Windows-Firewall und schränkt die Nutzung des USB-Ports ein.
- Am Web-Proxy (SWG) erfolgt die HTTP-Rückkanalkontrolle der Kommunikation von Schadcode zum Command & Control Center, inkl. SSL-Entschlüsselung.

4.3.2 BEISPIEL 2: FOKUS AUF „DEFAULT DENY“ UND „ASSUME BREACH“

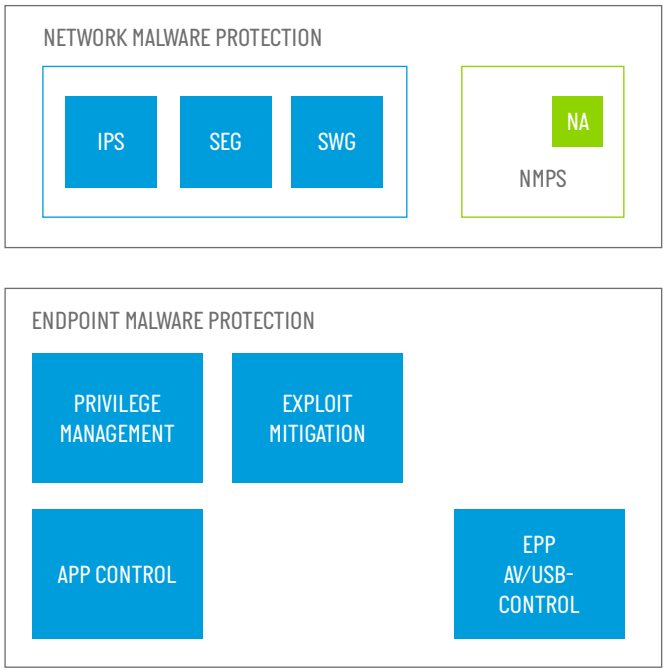

Abbildung 5: Beispiel 2

Wesentliche Architekturmerkmale:

- eine Klasse für alle Clients
- Application Control mit Whitelisting und Privilege Management mit Kaufsoftware
- MS EMET als Exploit Mitigation für erlaubte Anwendungen
- NMPS mit Netzwerkanalyse (NA) im Unternehmensnetzwerk für „breach detection“
- Eine klassische Endpoint Protection Suite (EPP) dient dazu, bekannte Malware mit minimalem Aufwand zu entfernen, steuert die Windows-Firewall und schränkt die Nutzung des USB-Ports ein (alternativ dazu Verwendung der Windows-Bordmittel).

+	0-Day – Prävention – Internet threats
+	Prävention – internal threats
++	Prävention – user miss behavior
+	0-Day – Detektion (payload)
+	Breach-detection
-	Reaktion
+	Geeignet für Notebook mit direktem Internetzugang
++	Kompatibilität
++	Geringe Performanceeinbußen, Ressourcenverbrauch
++	Anwenderkomfort

Abbildung 6: Beispiel 2 – Wirksamkeit

5. ANHANG

WIRKSAMKEIT DER MASSNAHMEN IM VERGLEICH

	0-Day – Prävention – Internet threats	Prävention – internal threats	Prävention – user miss behavior	0-Day – Detektion (payload)	Breach-detection	Reaktion	Geeignet für Notebook mit direktem Internetzugang	Kompatibilität	Geringe Performanceeinbußen, Ressourcenverbrauch	Anwenderkomfort
Exploit Mitigation	+	0	-	+	-	-	+	+	++	++
Application Containment ReCOBS	++	-	-	0	-	-	-	0	0	0
Application Containment Virtualisierung	+	-	-	+	-	-	+	+	0	0
Application Containment App-Sandbox	+	-	-	0	-	-	+	+	+	+
Application Containment Micro-Virtualisierung	++	-	-	++	+	-	++	+	++	++
Application Control/ Privilege Management	+	+	++	-	-	-	+	++	++	++
NMPS – PA mit Client-Assessment-Tool	-	0	-	++	-	+	0	++	++	++
NMPS – PA und NA mit Client-Assessment-Tool	-	0	-	++	+	+	0	++	++	++
ETDR	-	-	-	+	+	++	+	+	+	+

Abbildung 7

5.1 ÜBERSICHT ALLER KOMPONENTEN

Alle genannten Komponenten in einer Übersicht.

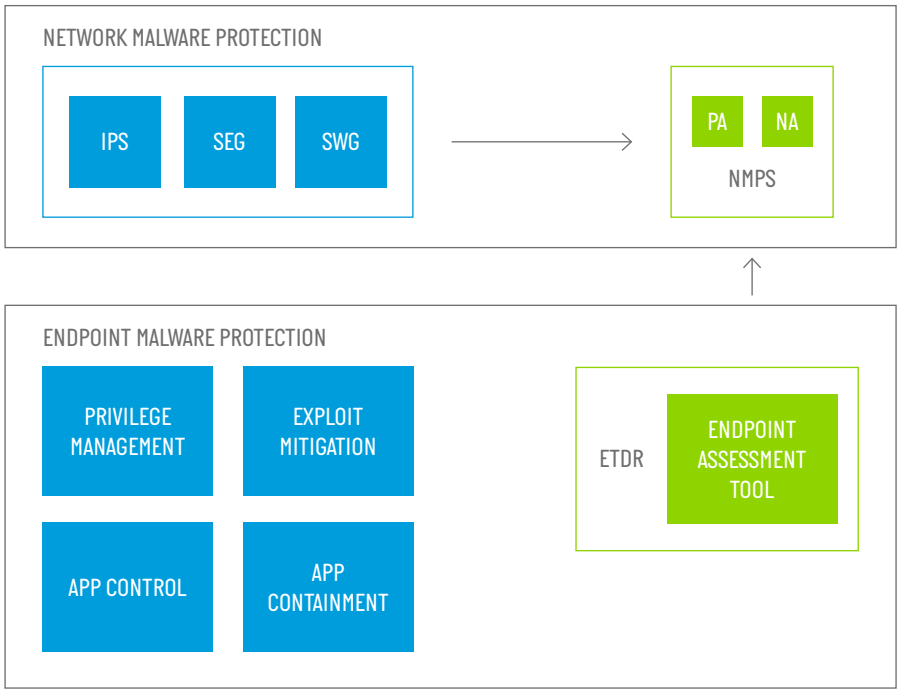

Abbildung 8: Advanced Endpoint Security – gesamt

5.2 KILL CHAIN

Verwendung hier gemäß „Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains"; Eric M. Hutchins, Michael J. Clopperty, Rohan M. Amin, Ph.D.z; Lockheed Martin Corporation

RECONNAIS-SANCE	WEAPONI-ZATION	DELIVERY	EXPLOITATION	INSTALLATION	COMMAND & CONTROL (C2)	ACTION
Research, identification and selection of targets, often represented as crawling Internet websites such as conference proceedings and mailing lists for email addresses, social relationships, or information on specific technologies.	Coupling a remote access trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer). Increasingly, client applications data files such as Adobe PDF or Microsoft Officedocuments serve as the weaponized deliverable.	Transmission of the weapon to the targeted environment using vectors like email attachments, websites and USB removable media.	After the weapon is delivered to victim host, exploitation triggers intruders' code. Most often, exploitation targets an application or operating system vulnerability, but it could also more simple exploit the users themselves or leverage an operating system feature that auto-executes.	Installation of a remote access trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.	Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel.	After progressing through the first six phases, can intruders take actions to achieve their original objectives. Typically this objective is data exfiltration which involves collecting, encrypting and extracting information from the victim environment. Alternatively, the intruders may only desire access to the initial victim box for use as a hop point to compromise additional systems and move laterally inside the network.

Computacenter

Computacenter AG & Co. oHG
Europaring 34–40, 50170 Kerpen

computacenter.de
+49 (0)2273 5970