CLOSING THE GAP IN MALWARE DETECTION

ERKENNUNGSALGORITHMEN REVOLUTIONIEREN

PANDA SECURITY

KURZBESCHREIBUNG

Panda Advanced Protection Service ist ein für jeden Kunden individualisierter und durch Panda gemanagter Security-Service. Die auf der Panda Collective Intelligence basierende Technologie dient speziell zur Abwehr von Targeted Attacks (Datendiebstahl) und **unbekannten** Bedrohungen, welche u.a. in hohem Maße Sicherheitslücken in vertrauenswürdigen Programmen ausnutzen. Dabei werden alle Prozesse (PEs) auf den Endpoints kontinuierlich überwacht und klassifiziert. Die forensischen Echtzeitanalysen liefern detaillierte Informationen über alle potenziell unerwünschten und gefährlichen Aktivitäten im Unternehmen.

Aufgrund von sowohl qualitativ als auch quantitativ ständig wachsenden Bedrohungen ist der Einsatz innovativer Technologien beim Schutz sensibler Daten alternativlos. Kriminelle und Entwickler von Sicherheitslösungen befinden sich in einem permanenten Wettstreit. Cyberkriminelle entwickeln ständig neue Angriffsszenarien, auf welche die Security-Industrie sowohl mit modernen Erkennungstechnologien als auch mit Blacklists antwortet.

Der Aufwand, den Unternehmen heutzutage betreiben müssen, um mit herkömmlichen Schutzlösungen ein kurzzeitig akzeptables Sicherheitsniveau zu erreichen, ist extrem ressourcen- und kostenintensiv. Panda Security's "Panda Advanced Protection Service" schließt genau diese Lücke in der Malwarebekämpfung. Dieser revolutionäre Ansatz, weg vom Blacklisting bekannter Bedrohungen, gewährleistet für Unternehmensnetzwerke ein permanent hohes Schutzniveau bei minimalem Aufwand.

Panda Security's innovative Technologie basiert auf drei Prinzipien:

1. Permanente Überwachung aller auf den Endpoints laufenden Prozesse.

2. Kontinuierliche Klassifizierung und Risikobewertung laufender Programme in Echtzeit.

3. Transparenz und Benutzerfreundlichkeit ohne administrativen Aufwand.

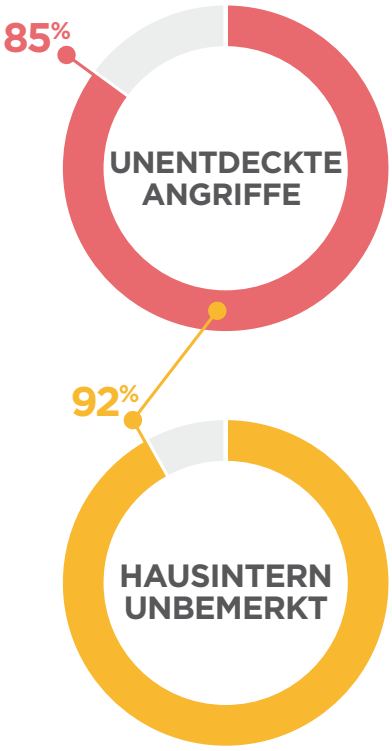
AKTUELLE BEDROHUNGSLAGE

Trotz ständig steigender Investitionen in die IT-Sicherheit (2013 gaben Unternehmen laut Gartner mehr als 13 Mrd. Dollar für Firewalls, Intrusion Prevention Systeme, Endpoint-Protection-Plattformen und sichere Web-Gateways aus) wird der Kampf gegen Cyberkriminalität immer komplexer und aufwändiger.

Groß angelegte Malware-Angriffe sowie bedeutende Enthüllungen über staatlich geförderte Spionageaktivitäten sorgen kontinuierlich dafür, dass das Infektionsrisiko durch Malware, speziell in Unternehmensnetzwerken, bewusster wahrgenommen wird.

Gartner hat die Gefahr erkannt: „Alle Unternehmen sollten jetzt davon ausgehen, dass sie sich in einem Zustand ständiger Gefährdung befinden." Angesichts des allgemeinen Widerwillens von IT-Abteilungen, Daten über Infizierungen und Sicherheitslücken zu veröffentlichen, lässt sich die heutige Situation mit den vergangenen Jahren nur sehr schwer vergleichen.

Niemand möchte Statistiken über seine Ausfallraten preisgeben. Laut des Verizon Data Breach Investigations Reports **blieben 85 % der Angriffe auf Unternehmens-netzwerke für Wochen oder sogar länger unentdeckt** und 92 % der Angriffe wurden von Unternehmen selbst nicht erkannt. Es ist deshalb sehr wahrscheinlich, dass das Gesamtrisiko in der Vergangenheit auf einem ähnlichen Niveau war. Wie Donald Rumsfeld einmal sagte: „gibt es Dinge, von denen wir nicht wissen, dass wir sie nicht wissen."



DIE ERKENNUNGSLÜCKE

Gartner-Analytiker Dan Blum fasste das Problem des bestehenden Kräftespiels zwischen Cyberkriminellen und der IT-Security-Industrie bereits 2007 in einem Bericht perfekt zusammen (Damals arbeitete er noch für die Burton Group, später wurde er von Gartner übernommen.):

Eine Unternehmensplattform und die Risiken, denen sie ausgesetzt ist, sind nie lange im Gleichgewicht; solange das Gleichgewicht besteht, sind die Risiken unter Kontrolle und den bösen Jungs wird ihr Zahltag verwehrt. Aber auch die Cyberkriminellen müssen ihre Familien ernähren, also entwickeln sie ständig innovative Möglichkeiten, um das Risikogleichgewicht zu stören. Sobald ein böser Junge einen neuen Angriff entwickelt, können sich andere böse Jungs um ihn scharen und in kürzester Zeit großen Schaden verursachen. Sobald das passiert, steigen die Kosten zur Beseitigung der Bedrohung schnell an, und die Hersteller von Sicherheitslösungen müssen neue Schutztechnologien entwickeln. Dieses Kräftespiel treibt den Sicherheitsmarkt dazu, sich ständig festigen zu müssen, aber nie gefestigt zu sein.
Dan Blum (Burton-Gartner).

Diese Schlussfolgerung ist heute genauso gültig wie vor sieben Jahren. Praktisch ist das Interesse der Investoren am Endpoint-Sicherheitsmarkt im vergangenen Jahr deutlich gestiegen. Einerseits entstehen viele neue Unternehmen, die ihre neuen Methoden vorstellen. Einige von ihnen werden bereits in der Aufbauphase von größeren Anbietern übernommen.

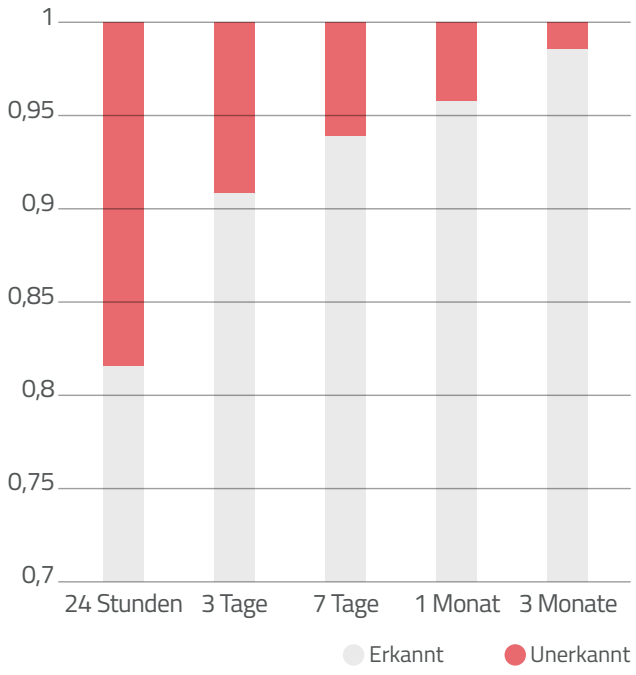
Andererseits entwickeln Cyberkriminelle permanent innovative Technologien zum Umgehen dieser neuen Sicherheitsmaßnahmen. Sie testen ihre neue Malware mithilfe der aktuellen Sicherheitsprodukte, die für die Suche nach schädlichen oder verdächtigen Codes herkömmliche Erkennungsalgorithmen nutzen. Ausschließlich Malware, die einer Entdeckung entgeht, wird von ihren Entwicklern verbreitet.

Auch Reputationssysteme bieten keine zuverlässige Absicherung. (Ein Reputationssystem vergibt aufgrund der Einschätzung einer Community oder Domain einen sogenannten Reputationsscore. Je höher der Score, desto vertrauenswürdiger die Software.) Neue Schadprogramme gelangen in die Systeme, indem sie deren Schwachstellen ausnutzen. Nutzen Sicherheitsanbieter eine zu aggressive Heuristik bei der Suche nach Malware, kann es zu sogenannten False-Positives kommen. **False-Positives werden** vom Markt **schwer bestraft**, deshalb streben die Anbieter eine Zero-False-Positive-Rate an. Dies führt allerdings nicht zur Maximierung der Leistungsfähigkeit von Schutzprogrammen. Laut Dan Blums Behauptung entwickeln die bösen Jungs letztendlich ständig neue Umgehungstechnologien. Das Ganze ist ein nie endender Prozess.

Von Januar bis Juni 2013 führten die PandaLabs eine interne Studie durch. Dabei wurden alle täglich gesammelten Malware-Exemplare mit einer großen Anzahl von Anti-Malware-Produkten getestet.

Das erschreckende Ergebnis dieser Studie: Ein ziemlich hoher Anteil der veröffentlichten Malware wird nicht rechtzeitig entdeckt. Fakt ist, dass auch ein Jahr nach Entdeckung der Malware fast 1 % der Exemplare immer noch unerkannt ist.

Von der AV-Industrie unerkannte Malware



Grafik. Erkennungslücke bei Anti-Malware-Produkten.

KOMPROMISSE BEI DER SICHERHEIT ELIMINIEREN

Gegen die immer neuen Angriffsszenarien entwickeln die Hersteller von IT-Sicherheitslösungen permanent neue Lösungen, die jedoch ebenfalls der bereits erwähnten Dynamik des „Reagierens" unterliegen.

Einige der neuen Lösungen arbeiten auf verschiedenen Ebenen der Infrastruktur (Endpoint, Netzwerkanalyse, netzwerkbasierte Appliances). Sie nutzen dabei unterschiedliche Technologien und erfüllen verschiedene Aufgaben (Prävention, Identifizierung, Recherche und Reaktion).

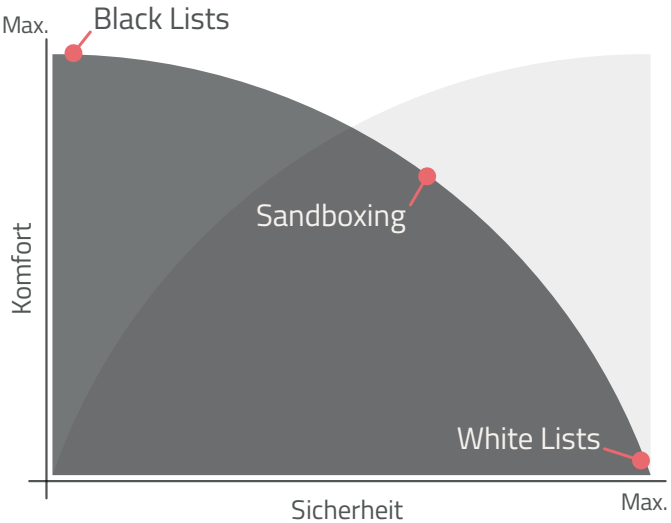
Die verantwortlichen Käufer von Sicherheitslösungen müssen nicht nur entscheiden, ob die neuen Lösungen in ihr Gesamtkonzept passen und den Schutzlevel erhöhen, ohne die Produktivität zu beeinträchtigen. Sie müssen ebenfalls die Gesamtkosten sowie die Benutzerfreundlichkeit bewerten und in Relation zueinander setzen.

Trotz übereinstimmender Meinungen, dass sie als Schutzmechanismen nicht mehr ausreichen, haben herkömmliche Antivirenlösungen jahrzehntelang die Endpoint-Sicherheitsbranche dominiert. Ihr Verbreitungsgrad ist aufgrund der Benutzerfreundlichkeit der höchste unter den Sicherheitsprodukten.

In den zurückliegenden Jahren wurden als Ergänzung zu den klassischen Antivirenprodukten insbesondere „Whitelisting" sowie „Application Control" empfohlen. Aufgrund des hohen administrativen Aufwands sowie der erhöhten Wartungskosten setzten sich diese Methoden jedoch nicht durch.

In den vergangenen 12 – 18 Monaten ist ein neuer Markt entstanden, der durch eine Mischung aus Lösungsansätzen und Technologien geprägt ist. Die verschiedenen Methoden reichen vom endpoint-basierten Eindämmen über Mikrovirtualisierung bis hin zur Nutzdatenanalyse mithilfe von Sandboxing. Jedoch können all diese Lösungen vorhandene Anti-Malware-Lösungen noch nicht vollständig ersetzen, da zusätzliche Investitionen notwendig sind. Außerdem basiert die Leistungsfähigkeit weiterhin auf denselben erkennungsbasierten Algorithmen, was eine Umgehung der Schutzmaßnahmen durch Cyberkriminelle ermöglicht.

Sicherheitskompromisse



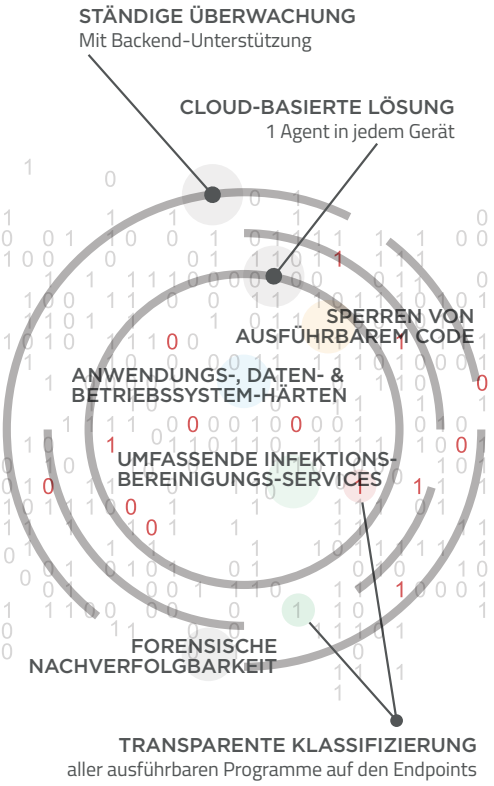
Grafik. Wie die Branche Malware bekämpft.

WAS IST PANDA ADVANCED PROTECTION SERVICE?

Panda Advanced Protection Service ist ein Managed Security-Service, der Malware zuverlässig erkennt, indem er alle laufenden Anwendungen automatisch und transparent überprüft.

Dieser Sicherheitsservice ist speziell für Unternehmenskunden konzipiert. Er besteht aus einer agenten- und cloud-basierten Lösung sowie einer ständigen Backend-Unterstützung durch Analysten der PandaLabs. Panda Advanced Protection Service klassifiziert transparent und mit dem höchsten Grad an Genauigkeit alle ausführbaren Programme (PE-Dateien) auf den Endpoints. Als weitere Basisschicht ermöglicht er ein Härten von Anwendungen, Daten und Betriebssystemen (Behavior Enforcement). So wird sichergestellt, dass häufig genutzte Anwendungen nicht aufgrund von Schwachstellen erfolgreich ausgenutzt werden können und dass auf sensible Bereiche des Betriebssystems nicht abnorm zugegriffen werden kann.

Des Weiteren erfolgt beim Eintreten eines Störfalles eine forensische Untersuchung, um Fragen nach dem Was, Wann, Wer und Wie des Malware-Angriffs detailliert beantworten zu können. Panda Advanced Protection Service kann ausführbaren Code sperren, bevor dieser zur Ausführung kommt (Extended Mode - Base Blocking Mode). Im Rahmen der optional erhältlichen Service-Pakete beinhaltet Panda Advanced Protection Service u. a. einen zusätzlichen Dienst zur vollständigen Desinfektion innerhalb des Netzwerkes.



DIE DREI PRINZIPIEN

Panda Advanced Protection Service basiert auf 3 Prinzipien:

Ständige Überwachung

Jeder Start einer ausführbaren Datei wird aufgezeichnet. Dies dient der Klassifizierung, Frühwarnung und Bewertung von ausführbaren Dateien im Klassifizierungssystem, der Nachverfolgbarkeit und der Störfallanalyse.

Ständige Klassifizierung laufender ausführbarer Dateien

Alle ausführbaren Dateien werden klassifiziert, bis ein maximaler Vertrauenslevel (MCL) erreicht ist (fast 100 %). Dazu werden sowohl lokale als auch cloud-basierte Systeme genutzt. Diese gleichen die Dateien mit lokal gesammelten Informationen sowie mit zahlreichen anderen kontextabhängigen Daten aus der Community mithilfe einer Big-Data-Analyse-Engine ab. Bei Bedarf kann auch eine manuelle Klassifizierung erfolgen.

Zudem müssen sich Programme entsprechend „verhalten", um ihre Vertrauenswürdigkeit zu bestätigen. Die Berechnungen zur Bestimmung des Vertrauenslevels basieren auf der firmeneigenen Clustering-Technologie sowie auf den empirischen Daten aller Dateien (Malware und Goodware), die in der Vergangenheit bereits von Panda klassifiziert wurden. Sobald neue Informationen vorliegen, erfolgt eine Neuberechnung durch eine nachträgliche Analyse aller vorherigen Klassifikationen.

Transparenz/Komfort

Weder Eingaben von Administratoren noch von Endanwendern (z. B. Erstellen von Whitelists, Konfiguration von Parametern usw.) sind für das Funktionieren des Services erforderlich. Sobald er installiert ist, kann der Agent ausführbare Dateien erkennen, analysieren und klassifizieren – sowohl selbstständig als auch in Verbindung mit dem System in der Cloud.

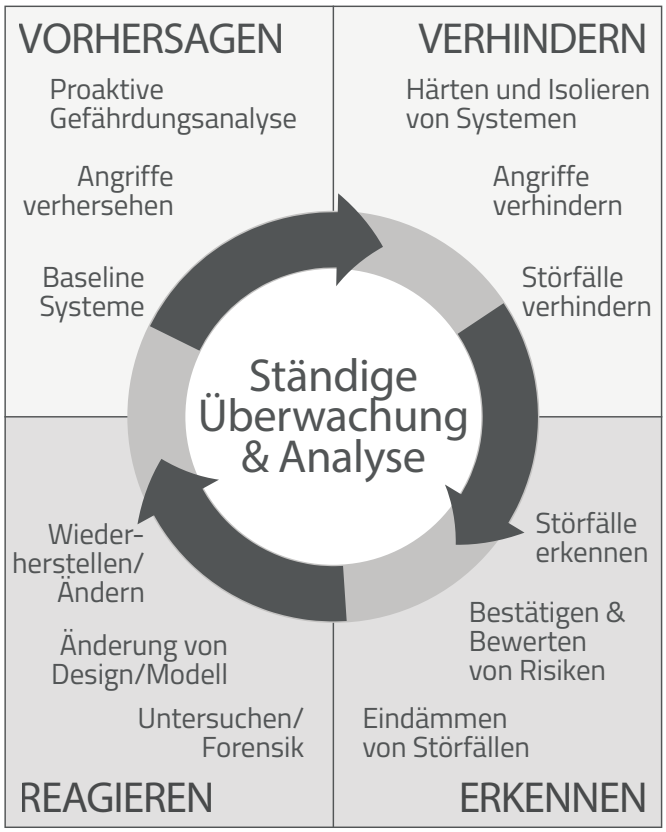
Panda Advanced Protection Service ist ein von Panda Security angebotener Managed Service, der Administratoren die Arbeit erheblich erleichtert, indem er Routineaufgaben übernimmt. Wenn Sicherheitslösungen von Drittanbietern genutzt werden, müssen Administratoren Warnmeldungen über verdächtige Aktivitäten selbst beurteilen und bearbeiten. Panda Advanced Protection Service überprüft jeden Verdacht umfassend und transparent. Administratoren erhalten anschließend Meldungen darüber, welche Anwendungen als Malware klassifiziert wurden.

Mit Panda Advanced Protection Service ist es nicht mehr erforderlich, Anwendungen auf eine Whitelist zu setzen oder Ausnahme- und Genehmigungsprozesse einzuführen, da alle ausführbaren Dateien vom System klassifiziert werden.

PANDA ADVANCED PROTECTION SERVICE & GARTNERS ANPASSUNGSFÄHIGE SICHERHEITSARCHITEKTUR

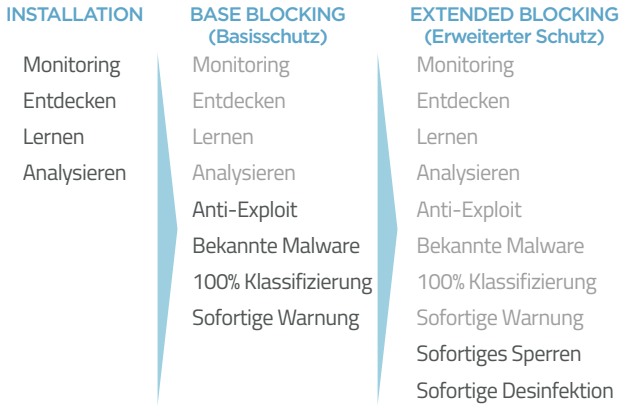
Panda Advanced Protection Service beinhaltet Analysetechnologien, um Malware-Aktivitäten zu blockieren, aufzudecken und zurückzuverfolgen. Ein neuer Bericht von Gartner „*Entwicklung einer anpassungsfähigen Sicherheitsarchitektur zum Schutz vor hochentwickelten Angriffen*" klärt über die Grenzen herkömmlicher Schutzkonzepte auf. Der Report empfiehlt Anbietern die Integration von 12 unterschiedlichen Technologien für einen effektiveren Schutz vor komplexen Bedrohungen.

Panda Advanced Protection Service umfasst bereits die Kernprinzipien dieser neuen Architektur, indem er ständig die Aktivitäten aller ausführbaren Programme auf den Endpoints überwacht. Außerdem führt er eine cloudbasierte Analyse der Informationen durch, die er in Echtzeit von Endpoints und zusätzlichen externen Quellen erhält.



Quelle: Gartner, Designing an Adaptive Security Architecture for Protection From Advanced Attacks, Neil MacDonald, February 2014

PHASEN



Installationsphase

I. Den Agenten installieren

Nach der optionalen Proxy-Konfiguration sollte der Agent (MSI-Paket oder exe-Datei) idealerweise auf allen Netzwerkgeräten installiert werden. Dabei sollten Active-Directory-Richtlinien, wenn verfügbar, angewendet werden. Mit den entsprechenden Administratorrechten kann der Agent auch mithilfe von Verteilsoftware installiert werden. Direkt nach der Installation meldet sich der PAPS-Agent beim Service an und sammelt sofort allgemeine Informationen über den Rechner. Dadurch wird eine eindeutige Zuordnung von Computer, Kunde und den auftretenden Ereignissen ermöglicht.

II. Vorfälle überwachen

Nach erfolgreicher Installation beginnt der Agent mit der Überwachung und Klassifizierung aller laufenden Prozesse, wie z. B.:

1. Dateidownloads
2. Softwareinstallation
3. URL zum Dateidownload
4. Modifikation der Hosts-Datei
5. Alter der Datei
6. Treibererstellung
7. Window hook/unhook
8. Prozesskommunikationen (IPs, Ports, Protokolle)
9. PE-Erstellung, Modifikation
10. DLL-Last
11. Service-Erstellung
12. PE-Mapping
13. Datei löschen/umbenennen
14. Ordnererstellung
15. Archiverstellung/Öffnen
16. Registry-Key-Erstellung/Modifikation
17. Pfaderstellung im Remote-Prozess
18. Prozess beenden
19. Zugriff auf den Security Accounts Manager (SAM)
20. Datenzugriff (mehr als 200 Dateiformate)

BETRIEBSARTEN

Base Blocking (Basisschutz)

Nach der Installationsphase, deren Dauer je nach Größe und Komplexität des Netzwerkes variiert, beginnt Panda Advanced Protection Service mit dem Schutz. Dazu erstellt er zuerst eine Basiskonfiguration zur Härtung, sodass:

I. Anwendungen wie Java, Flash, Microsoft Office und der verwendete Browser vor exploit-basierten Angriffen geschützt sind. Dabei werden kontextbezogene und verhaltensbasierte Regeln angewandt.

II. Daten und bestimmte sensible Bereiche des Betriebssystems gegen unerlaubten Zugriff von Drittanwendern geschützt werden. Der Zugriff auf Anwendungen, die während der Installationsphase analysiert und als legitim klassifiziert wurden, ist jedoch erlaubt.

III. Alle ausführbaren Programme mit einer Genauigkeit von nahezu 100 % (99,9999 %) klassifiziert werden. In dieser Betriebsart dürfen ausführbare Programme, die noch nicht mit einer MCL klassifiziert wurden, anfänglich laufen. Sobald das System ein Programm als Malware klassifiziert hat, wird die Ausführung sofort unterbunden.

Im Base-Blocking-Modus werden Endpoints gegen exploit-basierte Angriffe, die auf häufig genutzte Anwendungen abzielen, und gegen anomale Zugriffe auf Daten gehärtet. Erkennung, Bewertung und Eindämmung – alles wird automatisch vom System ausgeführt. Neue Malware wird durch die Klassifizierung aller ausführbaren Programme enttarnt. Wenn mehrere ausführbare Programme auf eine vollständige Klassifizierung warten, werden sie anhand ihrer Aktivitäten priorisiert. Dadurch wird das Risiko in allen Phasen kontrolliert. Die neue Malware wird dann eingedämmt und sämtliche Aktionen werden protokolliert. Alle gesammelten Informationen werden dem Administrator zur weiteren Analyse zur Verfügung gestellt.

Extended Blocking (Erweiterter Schutz)

Der Kunde kann auch den Extended-Blocking-Modus für einige oder alle Computer in seinem Netzwerk installieren. Der Extended-Blocking-Modus enthält dieselben Standardrichtlinien wie der Base-Blocking-Modus. Zusätzlich sperrt er jedes ausführbare Programm, das nicht automatisch mit einer MCL klassifiziert werden kann und zu starten versucht. Die Klassifizierung erfolgt gewöhnlich in wenigen Sekunden oder Minuten.

Wenn ein Programm gesperrt wurde, erhält der Endanwender eine Mitteilung darüber auf dem Bildschirm. Während der Installationsphase können zwei Arten von Usern eingestellt werden: einfacher User und VIP-User.

Einfache User können die Sperrung einer Anwendung nicht aufheben. Sie dürfen allerdings „protestieren", indem sie auf eine dafür vorgesehene Schaltfläche klicken. Diese persönliche Endanwendereinschätzung wird in das System als weitere zu berücksichtigende Information eingespeist.

Die VIP-User hingegen können die Sperrung eines Programmes aufheben. Wurde dieses Programm jedoch bereits als Malware klassifiziert, bleibt es gesperrt.

Reports und Warnmeldungen

In beiden Betriebsarten erhalten Administratoren zwei Arten von Reports:

- einen täglichen Aktivitätsreport, der Statistiken über die PAPS-Installation, angeschlossene Geräte, stark gefährdete Anwendungen usw. enthält
- sofortige Warnmeldungen bei jeder Klassifizierung von Malware.

Die Warnmeldung enthält einen forensischen Bericht über alle Aktionen, die von der Malware ausgeführt wurden, seit diese ins System gelangt ist. Der Bericht gibt ebenso an, von welcher URL sie heruntergeladen wurde (wenn das ein Infektionsvektor war), welche anderen Geräte im Netzwerk mit derselben Malware infiziert sind, welche ungeschützte Anwendung genutzt wurde, um das Netzwerk zu infiltrieren usw. Administratoren können über die Konsole auf diese Informationen zugreifen.

Foto. Panda Advanced Protection Service Dashboard.

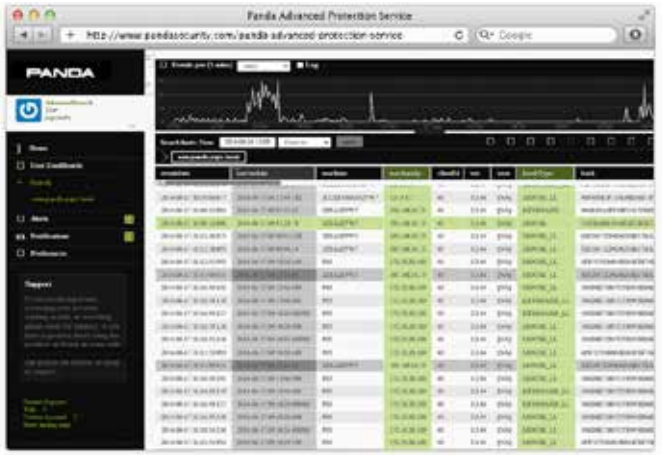


Foto. Panda Advanced Protection Service Events.

TECHNOLOGIE

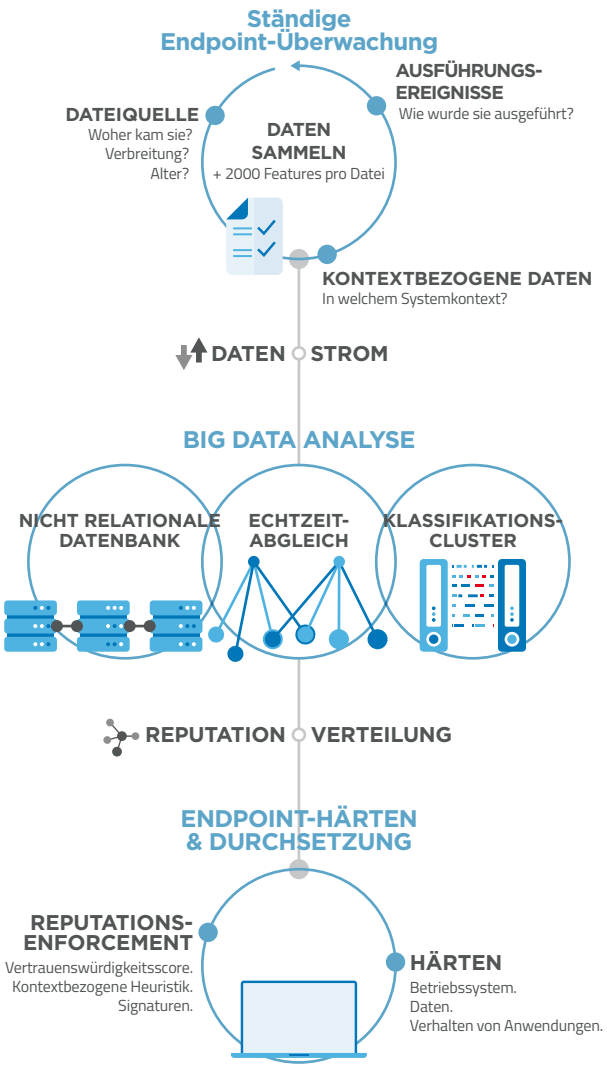


Abbildung. Big Data Analyse und Endpoint Enforcement

Panda Advanced Protection Service basiert auf einer Technologie, die sowohl interne als auch externe Informationsquellen einbezieht. Interne Informationen kommen von Endpoints. Externe Informationen sind z. B. Angaben zu Bedrohungen und zur Reputation von Anwendungen, Eingaben von Dritten und von Usern aus der Panda-Community.

Um alle Daten zu sammeln, abzugleichen und zu verarbeiten, werden sie in eine Big-Data-Analyse-Engine eingespeist und dann in einem Komponentensatz zusammengefasst. Das Endergebnis ist ein Klassifizierungscluster, den jede Datei durchlaufen muss, um eine Bewertung als „gut" oder „schlecht" mit einem „Maximalen Vertrauenslevel" (MLC) zu erhalten.

Das MLC gibt an, wie hoch die Wahrscheinlichkeit ist, dass eine Dateiklassifizierung (entweder Malware oder Goodware) korrekt ist. Dazu werden sowohl alle bisherigen empirischen Daten der PandaLabs über Malware- und Goodware-Exemplare einbezogen als auch neue Informationen.

Zur Bestimmung der Wahrscheinlichkeiten werden feststehende, kontextbezogene, verhaltensbezogene und externe Daten sowie eigenentwickelte hierarchische Clusteralgorithmen genutzt. Bei Bedarf werden zudem ausführbare Programme in einer physikalischen Umgebung (keine VMs) ausgeführt. Alle Programmdateien werden solange klassifiziert, bis das MCL erreicht ist. Sollten sie das MCL beim ersten Mal nicht erreichen, müssen sie weitere Klassifizierungsrunden durchlaufen. Dabei werden dann zusätzliche Filter- und Zuordnungsschichten genutzt. In Ausnahmefällen werden auch manuelle Analysen durchgeführt. Der grundlegende Aspekt dieser Vorgehensweise ist, dass keine ausführbare Datei ohne MCL-Klassifikation gestartet wird.

VORTEILE

Closing the Gap in Malware Detection

Schutz vor bekannter und unbekannter Malware (Viren, Trojaner, Spyware, etc.) sowie vor komplexen Bedrohungen.

Schutz vor exploit-basierten Angriffen auf Schwachstellen in häufig genutzten Anwendungen, wie z. B. Java, Microsoft Office, Adobe und diversen Browsern. Dieser Schutz entschärft das Risiko besonders in solchen Systemen, die aufgrund von internen oder externen Umständen schwer oder gar nicht zu patchen sind. Das gilt angesichts seines EOL (End of Life) insbesondere für Windows XP.

Schutz für Virtualisierte Desktopumgebungen.

Identifizierung von Anwendungen mit kritischen Schwachstellen.

Schutz vor anomalem Zugriff auf sensible Daten, Anwendungen und sensible Bereiche des Betriebssystems. Panda Advanced Protection Service schützt vor nicht vertrauenswürdigen Programmdateien, die auf Daten oder sensible Bereiche des Betriebssystems, wie z. B. den Security Accounts Manager (SAM), zugreifen oder Daten verschlüsseln wollen (wie z. B. die Cryptolocker Familie).

Minimierung der Wiederherstellungskosten im Störfall

Panda Advanced Protection Service gibt einen umfassenden Einblick in einen Störfall und liefert forensische Daten, die bei der Wiederherstellung und beim Schutz vor zukünftigen Angriffen hilfreich sind. PAPS erkennt infizierte Geräte, alle von der Malware ausgeführten Aktionen, den Eintrittszeitpunkt der Malware, den Infektionsvektor, die betroffenen Dateien usw.

Bereinigungshilfe im Falle einer Infektion. Im Rahmen eines zusätzlichen Services unterstützen Panda-Experten die PAPS-Kunden bei der kompletten Beseitigung einer Infektion und ihren Auswirkungen umfassend.

Transparenz ohne Managementinfrastruktur

Panda Advanced Protection Service basiert auf einem Agenten, der völlig transparent für Administratoren und Endanwender arbeitet. Er erfordert keine Installation oder Wartung von Servern, Datenbanken oder Konsolen.

FAZIT

In der aktuellen Situation sind herkömmliche erkennungsbasierte Algorithmen nicht ausreichend, um einen zuverlässigen Schutz zu gewährleisten. Cyberkriminelle veranstalten ein ständiges Wettrüsten, um eine vorübergehende Führung im Kampf gegen Entwickler von Sicherheitslösungen zu erlangen.

Eine neue Methode, die auf einem Agenten am Endpoint basiert und durch eine cloud-basierte Infrastruktur sowie die Hilfe von Sicherheitsexperten gestützt wird, ist zwingend erforderlich.

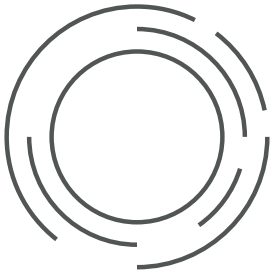
Panda Advanced Protection Service basiert auf drei Prinzipien:

1. Permanente Überwachung aller auf den Endpoints laufenden Prozesse.

2. Kontinuierliche Klassifizierung und Risikobewertung laufender Programme in Echtzeit.

3. Transparenz und Benutzerfreundlichkeit ohne administrativen Aufwand.

Panda Advanced Protection Service bietet die notwendigen forensischen Fähigkeiten, um im Falle einer Infektion zu reagieren, zu bestimmen, wann Malware das System infiltriert hat, wer betroffen war, was das Ziel war und wie sie dorthin gelangt ist.



CLOSING THE GAP IN MALWARE DETECTION

ERKENNUNGSALGORITHMEN REVOLUTIONIEREN

PANDA SECURITY