Marktübersicht: Neue Techniken der Endpoint-Security

Endstation Gerät

Stefan Strobel

Was einst mit trivialen Virenschutzprogrammen für Desktops angefangen hat, hat sich unter dem Schlagwort „Endpoint-Security“ zu komplexen Schutzmechanismen für alle erdenklichen Endpunkte und Geräte entwickelt. Der Markt ist in den letzten Jahren stark in Bewegung geraten.

Endpoint-Security ist ein Thema mit einer langen Geschichte, und dennoch ist es derzeit aktueller als in den letzten 15 Jahren. Von vielen Herstellern werden Produkte als „Next Generation“-Antivirus (AV), Anti-Malware oder schlicht „Endpoint-Security“ angeboten. In den letzten Jahren hat hier ein technischer Wandel stattgefunden, der von neuen Herstellern getrieben wurde, aber auch die etablierten dazu gebracht hat, ihre Lösungen stark zu erweitern. Wie überall in der IT spielen dabei Buzzwords wie „künstliche Intelligenz“, „maschinelles Lernen“ oder schlicht „Cloud“ eine wichtige Rolle.

Der größte Treiber des aktuellen Wandels ist die Diskussion über APTs (Advanced Persistent Threats), also gezielte professionelle Angriffe, die man mit klassischen signaturbasierten Antivirus-Techniken nicht verhindern kann. Viele Organisationen haben erkannt, dass signaturbasierter Virenschutz zu langsam und immer weniger wirksam geworden ist.

In Unternehmen ist Endgerätesicherheit heute mehr als nur der Schutz vor Malware. Auch die sichere Verbindung in ein Unternehmensnetzwerk über ein VPN, die Verschlüsselung lokal gespeicherter Daten, der Versuch, Datenabfluss zu verhindern, die Kontrolle von Schnittstellen wie USB oder die Kontrolle eingehender Kommunikation mit Firewall-Funktionen gehören neben vielen weiteren Sicherheitsfunktionen typischerweise zu Produkten in diesem Bereich dazu.

Die Ursprünge des Marktes für Endgerätesicherheit gehen dabei in die 80er-Jahre zurück, als Firmen wie McAfee, Symantec, Norman, Avira, G DATA und einige mehr erste Produkte zum Virenschutz entwickelt haben. Teilweise waren es auch einzelne Personen wie John McAfee oder Eugene Kaspersky, deren Namen schon damals mit Virenschutz assoziiert wurden.

Die Suche nach dem Muster

Die wichtigste Technik war ursprünglich die Suche nach bestimmten Mustern („Signaturen“) in Dateien. Diese Grundtechnik ist nach wie vor ein wesentlicher Bestandteil fast aller Virenscanner. Ihre Probleme liegen vor allem im technischen Fortschritt: Mit dem Wachstum des Internets und der zunehmenden weltweiten IT-Kompetenz gibt es auch immer mehr Kriminelle, die die IT und das Internet für sich entdeckt haben. Entsprechend gibt es immer mehr Malware, die täglich aufs Neue angreift. Gleichzeitig sind die Bandbreiten im Internet immer weiter ange-

wachsen, was die Verbreitung von Malware beschleunigt. Beides führt dazu, dass die Listen mit Signaturen, die ein Virenscanner benötigt, immer größer werden und eine neue Malware schneller verbreitet werden kann, als die Hersteller von AV-Lösungen ihre Signatur-Updates zu den Kunden bringen.

Klassischer signaturbasierter Virenschutz ist dadurch nicht generell schlecht, aber oft zu langsam. Malware wird dann weder zum Zeitpunkt der Infektion erkannt noch kann die Infektion verhindert werden. Auch der Ressourcenbedarf eines solchen AV-Systems wird durch das Wachstum der Signaturlisten größer, da immer mehr Signaturen vorgehalten und verglichen werden müssen.

Schon früh kamen erste Hersteller deshalb auf die Idee, andere, ergänzende Techniken in ein Schutzprodukt einzubauen oder komplementäre Produkte auf den Markt zu bringen. Der Versuch, Malware ergänzend zu Signaturen mit Heuristiken zu erkennen, ist ein Beispiel dafür. Bei dieser Methode wird eine Datei auf verdächtige, virentypische Eigenschaften überprüft.

Eine recht interessante Alternative kam um die Jahrtausendwende auf den Markt. Firmen wie Okena oder Platform Logic haben Produkte entwickelt, die jeden Zugriff eines Programms auf Ressourcen wie die Festplatte, die Registry, Netzwerkkommunikation, das Starten neuer Prozesse etc. überwachen und mit einem Regelwerk kontrollieren. Die Regeln definieren beispielsweise, dass ein Internetbrowser keine beliebigen anderen Programme starten darf, nur in bestimmte Verzeichnisse und Registry-Bereiche schreiben darf und so weiter. Diese Lösungen wurden „Host-based Intrusion Prevention System (HIPS)“ genannt.

Mit geeigneten Regeln kann ein HIPS verhindern, dass eine Malware Schaden auf einem Endgerät anrichtet und sich weiterverbreitet. Die Regeln müssen dabei auf die tatsächlich benötigten Programme angepasst werden. Signaturen oder Anpassungen an neue Malware sind dagegen nicht notwendig. Somit bietet ein HIPS

iX-TRACT

- Vor allem zwei Faktoren haben den Virenschutzmarkt in den letzten Jahren stark verändert: Zum einen die Tatsache, dass Microsoft mehr und mehr Schutzmechanismen teils kostenlos in seine Betriebssysteme integriert hat. Zum anderen die Erkenntnis, dass der klassische, auf Mustererkennung beruhende Virenschutz für heutige Angriffe nicht mehr ausreicht.
- Eine Sicherheitstechnik alleine bietet vor allem gegen sogenannte Advanced Persistent Threats keinen wirksamen Schutz. Heutige Produkte kombinieren verschiedene technische Ansätze.
- Wer ein Produkt zum Schutz seiner Endgeräte sucht, muss abwägen, ob er mit einem „Allrounder“ mit großer Abdeckung besser bedient ist oder ob es sinnvoller ist, mehrere Spezialisten gezielt zu kombinieren, deren Produkte in ihrem Spezialgebiet möglicherweise besser sind.

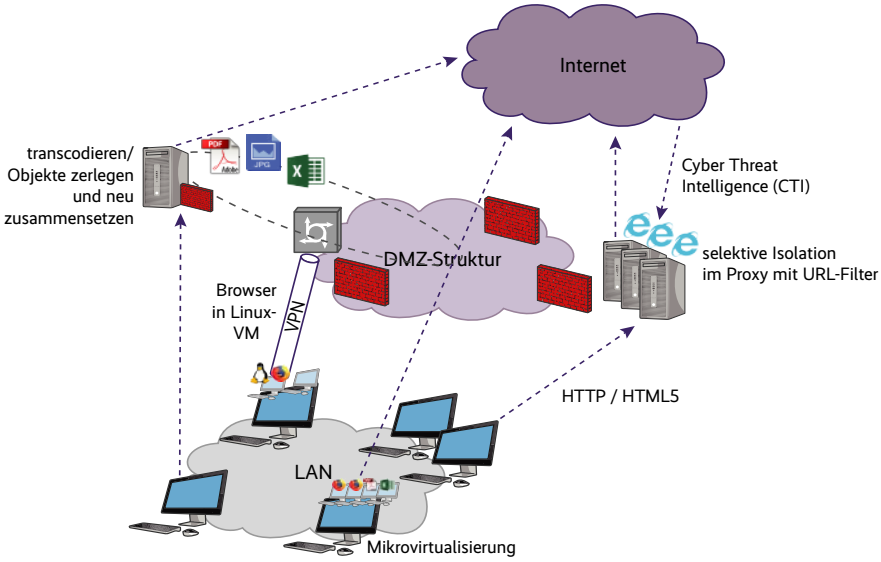
einen tatsächlich proaktiven und auch starken Schutz der Endgeräte.

Aus HIPS wird Verhaltenskontrolle

Problematisch ist allerdings die Komplexität und Menge der in der Praxis benötigten Regeln. Zudem kam die Technik zu einer Zeit auf den Markt, als noch Windows 98 und später Windows XP verbreitet waren. Diese Betriebssysteme hatten keine klaren Schnittstellen für derartige Sicherheitsprodukte, sodass sich ein HIPS mit Tricks an vielen Stellen in das Betriebssystem einklinken musste, was der Stabilität nicht gerade zuträglich war.

2003 wurde die Firma Okena von Cisco übernommen, die aus dem ursprünglichen Produkt den „Cisco Security Agent" machte, letztlich damit aber nicht erfolgreich war und ihn später einstellte. Platform Logic wurde von Symantec gekauft und teilweise in die existierende Lösung für Arbeitsplätze integriert. Für Server wurde daraus das Produkt „Symantec Critical System Protection". Auch McAfee kaufte einen HIPS-Player, die Firma Entercept.

Heute sind die Ideen von HIPS in vielen AV-Produkten integriert. Manchmal wird dafür auch noch der Name HIPS verwendet, manchmal ist nur von Verhaltenskontrolle die Rede. Auch Microsoft bietet für Windows 10 ähnliche Funktionen unter dem Namen „Attack Surface Reduction" an. Sie sind vor allem Bestandteil von „Windows Defender Advanced Threat Protection" und damit erst für Kunden mit einer E5-Lizenz, einer Unternehmensvolumenlizenz von Microsoft, verfügbar. Ein kleinerer Teil steht auch schon mit der günstigeren Microsoft-E3-Lizenz zur Verfügung.



Bei modernen Isolations-Gateways greift clientseitig ein normaler Browser per Proxy-Konfiguration auf einen vermeintlichen Proxy zu. Dieser holt sich die angefragte Webseite vom Server. Er reicht sie aber nicht 1 : 1 als HTML-Code durch, sondern rendert sie beispielsweise mit einer Chromium-Engine selbst und leitet sie als in HTML5 eingepacktes Bild an den anfragenden Browser zurück. Ein Anwender sieht also nur Bilder und kann durch Webseiten-Content nicht mehr angegriffen werden, da die Verarbeitung der Seite auf einem speziellen Sicherheitsgateway stattfindet (Abb. 1).

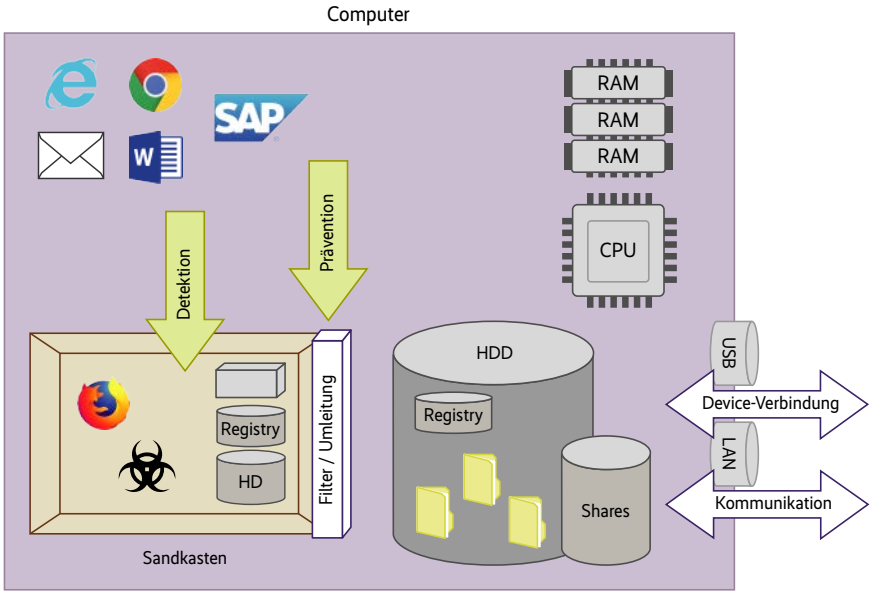
Noch älter als HIPS ist die Idee des „Application Whitelisting". Pioniere in diesem Bereich waren beispielsweise die Firmen SecureWave in den 90er-Jahren (heute Ivanti) und Bit9 (2002 gegründet, heute CarbonBlack). Ein Application-Whitelisting-System gestattet ausschließlich das Ausführen von Programmen, die explizit erlaubt (in einer Whitelist enthalten) sind. Der dadurch erreichbare Schutz vor Malware ist durchaus hoch, zumindest wenn die Malware als ausführbares Programm konzipiert ist oder ein solches nachlädt. Der Betriebsaufwand ist bei einer solchen Implementation aber auch sehr hoch.

Vom Whitelisting zur Signatur

Entsprechend hat sich die Technik weiterentwickelt und Bit9 war einer der ersten Anbieter, die das Ausführen von Programmen automatisch anhand sinnvoller Kriterien erlaubt haben. Kriterien waren dabei die digitale Signatur eines vertrauenswürdigen Herstellers oder der Weg, über den die Software installiert wurde.

Eine andere Umsetzungsvariante listet nicht mehr jedes zulässige Programm einzeln auf, sondern erlaubt nur noch das Starten von Programmen aus bestimmten Verzeichnisbäumen, die für den normalen Anwender nicht schreibbar sind. Somit kann ein Anwender eine aus dem Internet heruntergeladene Software nicht mehr starten, währen die normalen Programme unter C:\Programme etc. meist ohne Einschränkungen funktionieren.

Umsetzbar ist dieser Ansatz beispielsweise mit der AppLocker-Komponente von Microsoft, die seit Windows 7 kostenlos im Betriebssystem enthalten ist und von vielen Organisationen verwendet wird. Aber auch bei Windows XP gab es unter dem Namen Software Restriction Policies schon einen Vorläufer von AppLocker.

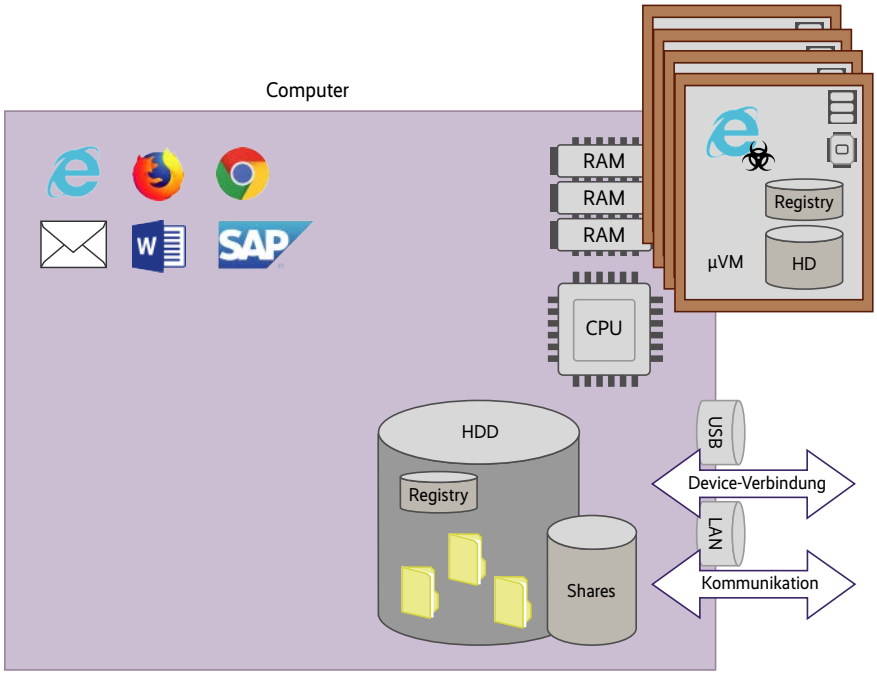


Browser und bestimmte andere Programme werden in einer Sandbox isoliert ausgeführt. Schreibende Zugriffe werden nur innerhalb der Sandbox vorgetäuscht. Das eigentliche Dateisystem dahinter wird nicht geändert (Abb. 2).

Eine gewisse Ähnlichkeit mit den früheren HIPS-Ideen haben moderne Ansätze zur Überwachung des Prozessverhaltens auf den Endgeräten. Bei ihnen überwacht ein Agent jede Aktivität eines laufenden Programms, jede Kommunikation und jeden Zugriff auf Ressourcen wie zum Beispiel Dateien oder Registry-Einträge. Im Gegensatz zu einem HIPS werden diese Aktivitäten jedoch nicht anhand einer Policy einzeln erlaubt oder blockiert, sondern das Verhalten wird im Verlauf analysiert, um bösartige Aktivitäten zu entdecken und dann darauf reagieren zu können.

KI bewertet Verhaltensmuster

Es geht dabei nicht um das Verhalten von Benutzern, sondern um technisches Verhalten der Prozesse. Wenn beispielsweise ein Prozess eine Datei aus dem Internet lädt, diese in einem Temp-Verzeichnis speichert, sie dann startet und wenn dann diese neu gestartete Datei noch Office-Dokumente verändert, dann wird es sich vermutlich um Malware handeln. Die Bewertung der Verhaltensmuster erfolgt oft mit KI-Methoden.



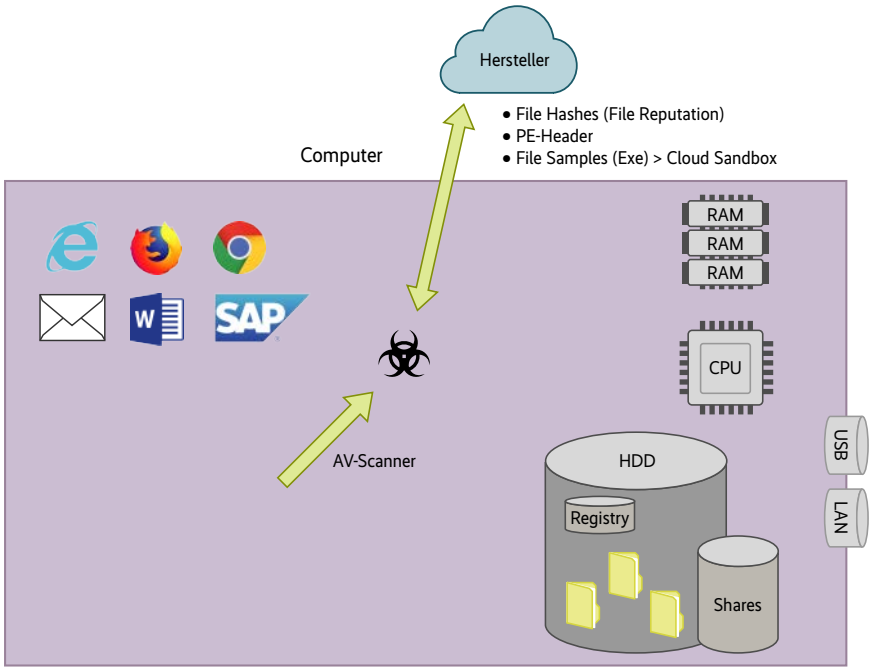
Jeder einzelne Task wie das Öffnen eines Mail-Attachments einer externen Mail oder einer externen Webseite im Browser wird in einer eigenen Mikro-VM gestartet (Abb. 3).

Bekannte Hersteller mit diesem Fokus sind beispielsweise SentinelOne, Sophos (durch Aufkauf von Invincea), Cybereason, CrowdStrike oder CarbonBlack. Auch Microsoft bietet eine Lösung zur Analyse des Prozessverhaltens unter dem Namen Defender ATP, die allerdings erst in einer E5-Lizenz enthalten ist. Bei manchen Produkten läuft das zentrale Management und die Analyse der einzelnen Events nur in der Cloud des Herstellers (beispielsweise bei Microsoft oder auch CrowdStrike),

während andere wie SentinelOne diese Funktion lokal im Netzwerk des Kunden vorhalten.

Analysten bezeichnen derlei Produkte meist als „Endpoint Detection and Response"-Lösungen (EDR), denn neben der Erkennung von Vorfällen spielt auch die Reaktion darauf eine wichtige Rolle. Einige Produkte können bösartiges Verhalten nicht nur erkennen, sondern bieten automatisches Reagieren wie das Stoppen des bösartigen Prozesses oder das Zurückrollen aller Änderungen, die der Prozess am System durchgeführt hat. Einige Hersteller bieten dem Sicherheitsexperten dann auch einen interaktiven Zugriff auf das System, um den Vorfall weiter zu untersuchen oder die Kompromittierung aufzuhalten.

Manche Produkte suchen aktiv nach weiteren kompromittierten Systemen anhand sogenannter „Indicators of Compromise" (IoCs). Man spricht dabei meist von „Threat Hunting". Solche Produkte helfen den Sicherheitsexperten bei der Suche, indem sie es beispielsweise sehr einfach und schnell im gesamten Netzwerk ermöglichen, weitere Systeme aufzuspüren, auf denen eine bestimmte Datei vorhanden oder ein bestimmter Registry-Key gesetzt ist.

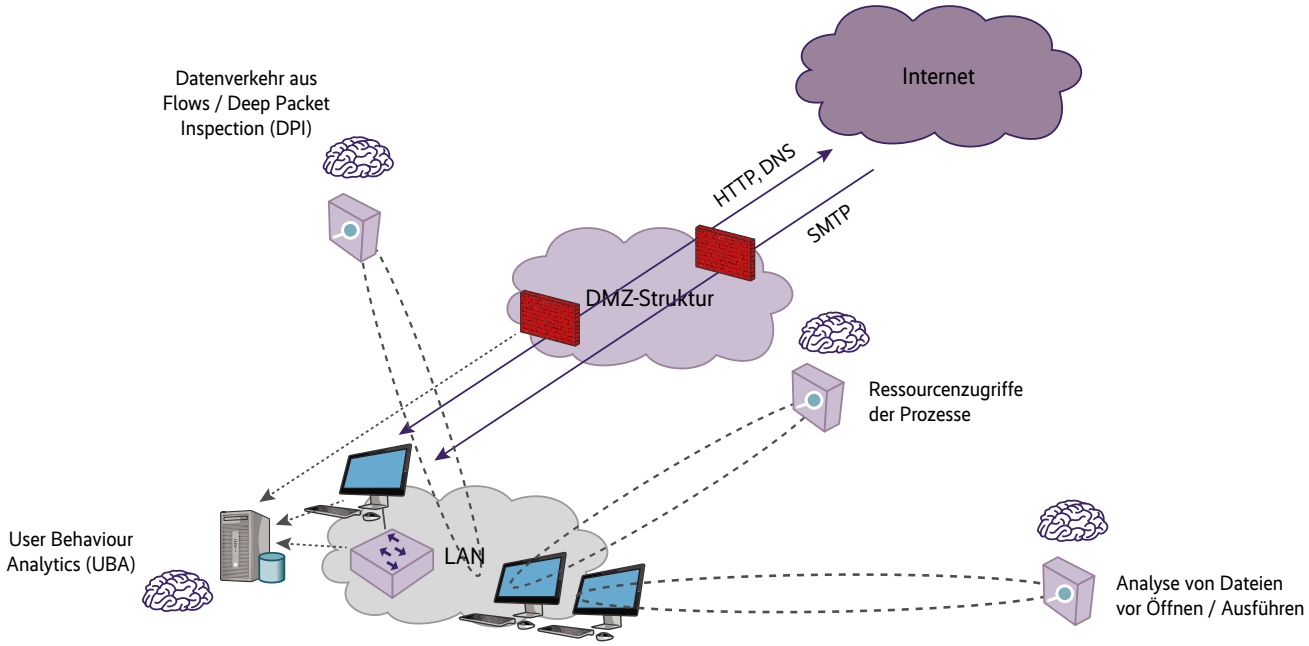


Die AV-Agenten fragen eine Klassifikation anhand von Hashwerten von Dateien in einer Datenbank des Herstellers ab. Darüber hinaus geben viele Hersteller bei nicht klassifizierten ausführbaren Programmen den PE-Header zur Analyse in die Cloud. Manchmal kann auch das ganze Programm zum Untersuchen in eine Sandbox in die Cloud geladen werden (Abb. 4).

Die Gefahren isolieren

Einen ganz anderen Weg gehen Isolationstechniken. Inspiriert von der ursprünglichen Idee, dass Internetnutzung auf einem dafür dedizierten zweiten PC neben dem normalen Arbeitsplatz stattfindet, haben sich verschiedene Techniken entwickelt (siehe Abbildung 1). Dabei benötigt man heute natürlich keinen zusätzlichen PC mehr. Stattdessen sollen potenziell gefährliche Aktivitäten per Software von den internen Applikationen und Daten isoliert werden. Dazu gehört das Surfen mit einem Webbrowser, aber oft auch das Öffnen von Dokumenten, die nicht aus dem eigenen Unternehmen stammen, sondern beispielsweise als Mailanhang von einem externen Absender empfangen wurden.

Eine schon recht lange existierende Isolationstechnik sind Sandboxes (siehe Abbildung 2). Eine Sandbox ist zunächst ein Bereich innerhalb des Betriebssystems, der Programme oder Prozesse isoliert und vom restlichen System abschottet.



KI kann an verschiedenen Stellen ansetzen: Dateien lassen sich vor dem Öffnen klassifizieren, zur Laufzeit kann eine Untersuchung des Prozessverhaltens erfolgen, außerdem lässt sich der Datenverkehr mit Machine Learning oder das Benutzerverhalten anhand der aufgezeichneten Logs analysieren (Abb. 5).

Hersteller von Endpoint-Security-Produkten

		Avira	Bitdefender	BlackBerry Cylance	CarbonBlack	Cisco	CrowdStrike	Cybereason	DriveLock	ESET	F-Secure	Fidelis	FireEye	G DATA
	Produkte	Avira Antivirus for Endpoint / Antivirus Pro	GravityZone Ultra	Cylance PROTECT, Cylance OPTICS	Predictive Security Cloud	Cisco AMP for Endpoints	Falcon	Cyber Defense Platform / EDR and Data Analytics	DriveLock Endpoint Protection	ESET Endpoint Security	F-Secure Protection Service for Business & F-Secure Business Suite	Fidelis Endpoint (ELEVATE Suite)	FirEye Endpoint Security	
	auf dem Markt seit	1988	2003	2014	2005 (Vorgänger)	2010	2013	2014	2002	1992	1988	2008	2014	1987
Malwareklassifikation	signaturbasiertes AV	✓	✓	–	✓	✓	–	✓	–	✓	✓	✓	✓	✓
	File-Klassifikation mit KI auf dem Endgerät	–	✓	✓	✓	✓	✓	✓	–	✓	–	–	✓	✓
	Analyse in der Cloud (Reputationscheck, KI für Header, KI für File, Sandbox)	– / – / ✓ / ✓	✓ / ✓ / – / ✓	✓ / – / –	✓ / – / (✓) / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / – / ✓	✓ / – / – / –	–	✓ / ✓ / ✓ / ✓	✓ / – / ✓ / ✓	✓ / – / – / –	– / – / – / Integration eigener Sandbox-Analyse-Lösung	✓ / – / ✓ / ✓
Kommunikation	eigene lokale Firewall	–	✓	–	–	(✓)	–	–	–	✓	–	–	–	✓
	Analyse der Kommunikation (Muster, IP-Adressen, Domains)	–	✓ / ✓ / ✓	– / – / –	– / ✓ / –	✓ / ✓ / –	✓ / ✓ / ✓	– / ✓ / ✓	–	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓
Exploit-Schutz	Exploit-Mitigation-Funktionen (Buffer-Overflows, Heap, ROP, Prozesse)	–	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	(✓) / (✓) / (✓) / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	–	–	✓ / ✓ / ✓ / ✓	– / – / – / ✓	–	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓
	Einschränkungen für Office-Makros (Starten von Programmen, weitere)	–	✓	✓	✓	(✓)	✓	–	–	✓	✓	✓	✓	✓
	Einschränkungen für PowerShell	–	✓	✓	✓	(✓)	✓	✓	–	✓	✓	k. A.	teilw.	✓
	Kontrolle des schreibenden Zugriffs auf Office-Dateien	–	✓	✓	–	–	✓	–	–	–	–	–	–	✓
Prozessverhaltensanalyse	Prozessverhaltensanalyse (Prozesse, Dateien, Registry, Kommunikation, Verschlüsselung)	–	✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ / ✓ k. A. Cylance Optics	✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / – / ✓ / ✓ Cloud-basiert	✓ / ✓ / ✓ / ✓ / ✓ Cloud-basiert	✓ / ✓ / ✓ / ✓ / ✓	–	✓ / ✓ / ✓ / ✓ / ✓	separates EDR-Produkt	✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ / ✓
	grafische Darstellung des Prozessverhaltens	–	✓	✓ Cylance Optics	✓	✓	✓	✓	–	✓	✓	✓	✓	–
	Rollback von erkanntem bösartigem Verhalten	–	✓	–	–	–	–	–	–	–	–	–	k. A.	✓
URL-Filter	Anzahl der vorgegebenen Kategorien	13	45	–	–	–	–	–	–	141	14–16	–	–	61
IoCs	bereits integrierte IoC-Feeds (Feed-Quellen)	–	k. A.	–	Mitre, Tor-Nodes, eigene Feeds	–	eigener IoC-Feed	eigene IoC-Feeds, enthält auch Virustotal	–	–	separates EDR-Produkt	eigene IoC-Feeds, Mandiant, IoC-Bucket und weitere	eigene IoC-Feeds	k. A.
	Nach welchen Arten von IoCs kann gesucht werden (z. B. File Hashes, Registry-Einträge, IP-Adressen …)?	–	✓ / – / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / – / ✓	–	✓ / ✓ / ✓	–	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / – / –

	HP (Bromium)	Ivanti	itWatch	Kaspersky	McAfee	Microsoft	Palo Alto	Panda Security	RSA	Sentinel-One	Sophos	Symantec	Threat-Locker	Trend Micro
	Bromium Secure Plattform	Ivanti Security Controls	itWatch Enterpise Security Suite itWESS, itWash-i	Kaspersky Endpoint Security	McAfee Endpoint Security + DER	Defender AV, Defender ATP	Traps	Adaptive Defense 360	NetWitness Endpoint	Sentinel-One Complete	Intercept X Advanced	Symantec Endpoint Protection	Threat-Locker Application Control	Smart Protection for Endpoint / Apex One
	2014	1991	1998	1997	1987	2006	2015	1996	2012	2014	1988	2007	2015	1988
	–	–	–	✓	✓	✓	–	✓	(✓)	–	✓	✓	–	✓
	–	–	–	✓	✓	✓	✓	✓	–	✓	✓	✓	–	✓
	–	–	–	k. A. / ✓ / ✓ / ✓	✓ / – / – / – Sandbox: Zusatzprodukt	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ integriert in Wildfire	✓ / ✓ / ✓ / ✓	✓ / – / – / – Sandbox Zusatzprodukt	✓ / – / – / –	✓ / ✓ / ✓ / ✓	✓ / – / – / ✓	–	✓ / ✓ / – / –
	–	teilw. (für Winsock)	–	✓	✓	Windows-Firewall	–	✓	–	Management der OS-Firewalls	Management der Windows-Firewall	✓	✓	✓
	–	–	–	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	–	✓ / ✓ / ✓	✓ / ✓ / ✓	–	✓ / ✓ / ✓	✓ / ✓ / ✓	–	✓ / ✓ / ✓
	–	–	–	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ ✓	✓ / ✓ / ✓ / ✓ Exploit Guard	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	–	–	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	–	✓ / ✓ / ✓ / ✓
	–	–	✓	✓	✓	Exploit Guard	✓	✓	–	–	✓	✓	(✓)	✓
	–	–	✓	✓	✓	Exploit Guard	✓	✓	–	–	✓	✓	(✓)	✓
	–	–	✓	✓	✓	Exploit Guard	✓	✓	–	–	✓	✓	✓	–
	✓ / ✓ / ✓ / ✓ / ✓ (in einer Micro-VM)	–	✓ / ✓ / ✓ / – / ✓	✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ / ✓ Cloud-basiert, Defender ATP	✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ / ✓	separates EDR-Produkt	✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / ✓
	✓	–	–	✓	separates EDR-Produkt	✓	separates Produkt (Cortex XDR)	✓	✓	✓	✓	separates EDR-Produkt	–	✓
	✓ Isolation	–	✓	✓	✓	✓	–	–	–	✓	✓	separates EDR-Produkt	–	✓
	–	–	–	14	105	–	–	64	–	–	50	separates Produkt	–	–
	–	–	–	–	–	eigener IoC-Feed, Schnittstellen	eigene IoC-Feeds	–	eigene IoC-Feeds	–	eigene IoC-Feeds	eigener IoC-Feed	–	ZDI, Sans, eigene
	–	–	–	✓ / ✓ / ✓ separates EDR-Produkt	✓ / ✓ / ✓	✓ / – / –	separates Produkt (Cortex XDR)	–	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	–	✓ / ✓ / ✓

Hersteller von Endpoint-Security-Produkten

		Avira	Bitdefender	BlackBerry Cylance	CarbonBlack	Cisco	CrowdStrike	Cybereason	DriveLock	ESET	F-Secure	Fidelis	FireEye	G DATA
USB	Blockieren von USB: generell / nach Geräteklassen	–	✓ / ✓	✓ / ✓	separates Produkt	–	✓ / ✓	–	✓ / ✓	✓ / ✓	✓ / ✓	über Skripte	–	– / ✓
	spezielle Features zum Schutz vor BadUSB- / RubberDucky-Angriffen	–	–	–	–	–	✓	–	–	–	–	–	–	separates kostenloses Produkt Keyboard Guard
	automatisches Verschlüsseln von Dateien, die auf USB-Sticks kopiert werden	–	–	–	–	–	–	–	✓	separates Produkt	–	–	–	–
Application Whitelisting	anhand von Pfaden auf der Festplatte, Hashwerten, Signaturen	–	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / –	–	–	✓ / ✓ / ✓	–	–	–	–	✓ / ✓ / ✓
Plattenverschlüsselung	Verschlüsselung der Festplatte	–	✓	–	–	–	–	–	✓	separates Produkt	–	–	–	–
	inkl. Pre-Boot-Authentisierung	–	✓	–	–	–	–	–	✓	separates Produkt	–	–	–	–
VPN	unterstützte VPN-Protokolle	–	–	–	–	separates Produkt	–	–	–	–	separates Produkt	–	–	–
	explizit unterstützte VPN-Gateway-Produkte	–	–	–	–	separates Produkt	–	–	–	–	separates Produkt	–	–	–
Isolation	lokale Sandbox zur Isolation von Webbrowser, Office-Programmen, Bildbetrachtern	–	–	–	–	–	–	–	–	–	–	–	–	–
	Mikrovirtualisierung zur Isolation von Webbrowser, Office-Programmen, Bildbetrachtern	–	–	–	–	–	–	–	–	–	–	–	–	–
DLP	konfigurierbare DLP-Policy für Inhalte abhängig von Dateitypen, Pfaden, Inhalten, Mailadressen	–	–	–	–	–	–	–	✓ / ✓ / – / –	–	–	separates DLP-Produkt	–	–
	Kontrolle für Copy / Paste	–	–	–	–	–	–	–	–	–	–	separates DLP-Produkt	–	–
	Reaktionen auf Verstoß gegen die DLP-Policy – Blockieren, Loggen, Begründung abfragen	–	–	–	–	–	–	–	✓ / ✓ / ✓	–	–	separates DLP-Produkt	–	–
Sanitisation / „Datenwäsche“	für Office-Dokumente, Bilder, PDF	–	–	–	–	–	–	–	–	–	–	–	–	–
	automatisches Entfernen von Makros bei eingehenden Office-Dokumenten	–	–	–	–	–	–	–	–	–	–	–	–	–
	generelle Konvertierung in PDF	–	–	–	–	–	–	–	–	–	–	–	–	–

	HP (Bromium)	Ivanti	itWatch	Kaspersky	McAfee	Microsoft	Palo Alto	Panda Security	RSA	SentinelOne	Sophos	Symantec	ThreatLocker	Trend Micro
	–	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	Defender ATP	–	✓ / ✓	–	✓ / ✓	– / ✓	✓ / ✓	✓ / ✓	✓ / ✓
	–	✓	✓	✓	–	–	–	(✓)	–	–	–	–	–	–
	–	✓	✓	✓	separates Produkt	BitLocker	–	–	–	–	separates Produkt	separates Produkt	–	✓
	–	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	AppLocker / Windows Defender Exploit Guard Application Control	–	✓ / ✓ / ✓	–	–	nur Server / ✓ / –	✓ / ✓ / –	✓ / ✓ / ✓	✓ / ✓ / ✓
	–	–	–	✓	separates Produkt	BitLocker	–	✓	–	–	separates Produkt	separates Produkt	–	✓
	–	–	–	✓	separates Produkt	✓	–	✓	–	–	separates Produkt	separates Produkt	–	✓
	–	–	–	–	–	IKEv2, L2TP, PPTP, SSTP	separates Produkt	–	–	–	separates Produkt	separates Produkt	–	–
	–	–	–	–	–	k. A.	separates Produkt	–	–	–	separates Produkt	separates Produkt	–	–
	–	–	✓ / ✓ / ✓ / ✓	–	–	(Windows Sandbox)	–	–	–	–	✓ / ✓ / – / ✓	–	–	–
	✓ / ✓ / ✓	–	–	–	–	Windows Defender Application Guard (nur für den Browser)	–	–	–	–	–	–	–	–
	–	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	–	separates DLP-Produkt	k. A. / ✓ / ✓	–	–	–	–	✓ / – / ✓ / –	✓ / ✓ / ✓ / ✓ separates DLP-Produkt	✓ / ✓ / ✓ / ✓ / –	✓ / – / ✓ / –
	–	–	✓	–	separates DLP-Produkt	✓	–	–	–	–	–	✓ separates DLP-Produkt	–	✓
	–	✓ / ✓ / –	✓ / ✓ / ✓	–	separates DLP-Produkt	✓ / ✓ / –	–	–	–	–	✓ / ✓ / ✓	✓ / ✓ / ✓ separates DLP-Produkt	✓ / ✓ / –	✓ / ✓ / –
	–	–	✓ / ✓ / ✓	–	–	–	–	–	–	–	–	separates Gateway-Produkt	–	–
	–	–	✓	–	–	–	–	–	–	–	–	separates Gateway-Produkt	–	–
	–	–	✓	–	–	–	–	–	–	–	–	separates Gateway-Produkt	–	–

Hersteller von Endpoint-Security-Produkten

		Avira	Bitde-fender	Black-Berry Cylance	Carbon-Black	Cisco	Crowd-Strike	Cybe-reason	DriveLock	ESET	F-Secure	Fidelis	FireEye	G DATA
zentrales Management	Management über GPOs / eig. Server / Coud-Service	über Dritt-produkte	✓ / ✓ / ✓	✓ / ✓ / ✓	– / – / ✓	–	– / – / ✓	– / ✓ / ✓	✓ / ✓ / ✓	– / ✓ / ✓	k. A.	–	– / ✓ / ✓	– / ✓ / ✓
	zentrale Sammlung aller Events / Logs	über Dritt-produkte	✓	✓	✓	✓	✓	✓	✓	✓	k. A.	✓	✓	✓
	Rollen- und Rechtekonzept	über Dritt-produkte	✓	✓	✓	✓	✓	✓	✓	✓	k. A.	✓	✓	✓
	Mandanten-fähigkeit	über Dritt-produkte	✓	✓	✓	✓	✓	–	✓	✓	k. A.	–	–	✓
	Zugriff auf AD-Gruppen	über Dritt-produkte	✓	✓	–	✓	–	✓	✓	✓	k. A.	✓	✓	–
	Anmeldung mit Zwei-Fak-tor-Authenti-sierung mög-lich	–	✓	✓	✓	✓	✓	✓	✓	✓	k. A.	✓	✓	–
	Schnittstelle zu SIEM-Syste-men	–	✓	✓	✓	✓	✓	✓	✓	✓	k. A.	✓	✓	–
	Export von Threat Intelli-gence per STIX/TAXII/ OpenIOC möglich	–	–	nur API	–	– / – / ✓	✓	–	–	✓	k. A.	–	– / – / ✓	–

Tabelle beruht weitgehend auf den Angaben der Hersteller; ✓: ja / trifft zu; –: nein / trifft nicht zu; k. A.: keine Angabe; ( ): eingeschränkt

Das soll verhindern, dass Schadcode das Betriebssystem manipuliert. Man kennt Sandboxes heute vor allem vom Java-Interpreter, von Android und iOS. Auch in der IT-Sicherheit gab es schon vor über 15 Jahren Sicherheitslösungen für Windows-Arbeitsplätze, die das Surfen im Internet oder das Verarbeiten von Mails dauerhaft innerhalb einer Sandbox isolierten.

Technisch klinken sich solche Produkte in nahezu alle Betriebssystemaufrufe ein. Im Gegensatz zu einem HIPS werden unerwünschte Schreibzugriffe jedoch nicht blockiert, sondern so umgeleitet, dass die Änderungen in einem eigenen Speicherbereich der Sandbox vorgehalten werden. Das Programm innerhalb der Sandbox meint somit, dass es beliebige Änderungen am System und an Dateien durchführen kann. In Wahrheit werden die Änderungen jedoch nur simuliert und die echten Zieldaten bleiben unverändert.

Die Sandbox-Produkte von vor 15 Jahren wie beispielsweise eSafe Enterprise von der Firma Aladdin oder Surfin Shield Corporate von Finjan waren damals ihrer Zeit voraus, existieren schon lange nicht mehr und sind vermutlich in Vergessenheit geraten. Von Finjan gibt es jedoch noch eine Nachfolgefirma, die die Patente von damals besitzt und von Firmen, die heute Sandbox-Techniken vermarkten, Lizenzgebühren einfordert.

Angreifbare Sandboxes

Die Schwachstelle von Sandboxes auf dem Endgerät ist vor allem, dass ein professioneller Angreifer das „Hooking“, mit dem sich die Sandbox typischerweise in die Betriebssystemaufrufe der isolierten Programme einklinkt, rückgängig machen kann. Zudem können Schwachstellen im Betriebssystemkern zu einem Ausbruch aus der Sandbox verwendet werden. Die Wirksamkeit einer Sandbox gegen professionelle Angriffe ist damit begrenzt.

Ein ganz anderer Anwendungsfall von Sandboxes sind Systeme, die lokale oder im Netzwerk übertragene Dateien für einen kurzen Zeitraum innerhalb einer Sandbox analysieren, um dadurch Malware an ihrem Verhalten zu erkennen. Dabei findet keine dauerhafte Isolation bestimmter Programme statt, sondern die Sandbox ist nur ein Hilfsmittel für die Analyse. Professionelle Malware ist jedoch oft in der Lage, solche Systeme zu umgehen. Dazu kommt noch, dass die Sandbox-Analyse nur für einen kurzen Zeitraum läuft. Dadurch kann Malware, die in dieser Zeitspanne nicht als verdächtig auffällt, nach der Analysephase ohne Einschränkungen durch die Sandbox Schadfunktionen ausführen. Hier müssen dann andere Features der Sicherheitsprodukte einschreiten.

Eine sehr ähnliche Grundidee wie Sandboxes auf Endgeräten lässt sich mit Mikrovirtualisierung implementieren (siehe Abbildung 3). Dabei wird technisch jeder zu isolierende Task in einer eigenen virtuellen Maschine eingesperrt, die per „Copy on Write“ nur als Differenz zu einer Kopiervorlage im Hauptspeicher existiert. Die Isolation ist dadurch deutlich stärker als bei Sandboxes. Neben der Firma Bromium, die als Pionier dieser Technik gilt und im September 2019 von HP übernommen wurde, setzt auch Microsoft stark auf Mikrovirtualisierung und in Windows 10 erscheinen immer mehr Features auf dieser Grundlage.

Geräte unter Kontrolle

Einen ganz anderen Angriffsvektor adressiert die Device-Kontrolle, eine Technik, die sich auf bestimmte Schnittstellen konzentriert, vor allem USB, und diese Schnittstellen entweder vollständig sperrt oder selektiv für bestimmte Geräte oder Inhalte öffnet. So lässt sich unterbinden, dass fremde USB-Sticks an einen Arbeitsplatz angeschlossen werden und Malware über diesen

	HP (Bromium)	Ivanti	itWatch	Kaspersky	McAfee	Microsoft	Palo Alto	Panda Security	RSA	Sentinel-One	Sophos	Symantec	Threat-Locker	Trend Micro
	– / ✓ / ✓	– / ✓ / –	✓ / ✓ / ✓	✓ / ✓ / –	– / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	– / – / ✓	✓ / ✓ / –	– / ✓ / ✓	– / – / ✓	– / ✓ / ✓	✓ / – / ✓	✓ / ✓ / ✓
	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	k. A.	✓
	✓	k. A.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	✓	k. A.	✓	✓	✓	✓	–	✓	✓	✓	✓	✓	✓	teilw.
	✓	k. A.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	–	k. A.	✓	über Azure AD	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	✓	k. A.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	✓ / k. A. / –	k. A.	–	–	bei ATD	k. A.	–	–	✓	–	–	STIX über EDR-Produkt	(✓)	✓

Weg auf einen PC gelangt. Ebenso kann man verhindern, dass vertrauliche Daten auf einen USB-Stick kopiert werden. Je nach Hersteller ist dabei die Grenze zu DLP-Produkten (Data Leakage Prevention), die den Abfluss vertraulicher Daten auf mehreren Wegen verhindern wollen, fließend.

Da viele Anwender USB-Sticks zum Austausch von Dateien regelmäßig benötigen, bringt das Sperren von USB-Ports jedoch auch Probleme mit sich. In der Praxis kann das dazu führen, dass es einerseits viele Ausnahmegenehmigungen gibt oder andererseits Anwender dazu verleitet werden, vertrauliche Dateien unverschlüsselt per Mail zu verschicken. Ein USB-Stick wäre dabei manchmal das kleinere Übel.

Cloud spart Zeit und Ressourcen

Eine Sonderfunktion, die nur wenige Hersteller anbieten, ist der Schutz vor Angriffen, bei denen ein vermeintlich harmloses USB-Gerät eine zusätzliche Tastatur simuliert und so bösartige Befehle an den Computer sendet. Die Malware ist dabei zum Beispiel Teil der Firmware eines USB-Geräts. Um vor solchen Angriffen zu schützen, kann ein Endpoint-Security-Produkt zum Beispiel beim Anschluss einer zweiten Tastatur zunächst den Benutzer fragen, ob er bewusst eine weitere Tastatur angeschlossen hat oder eigentlich nur einen Speicherstick.

Ergänzend oder als Alternative zu den herkömmlichen signaturbasierten AV-Ansätzen nutzen immer mehr Hersteller Cloud-basierte Funktionen (Abbildung 4). Das ist im einfachsten Fall die Onlineabfrage von Bewertungen beziehungsweise Reputationen zu Dateien. Dabei fragt ein Agent auf dem Endgerät beispielsweise mit dem Hashwert einer neuen Datei eine Datenbank in der Cloud ab. In dieser Datenbank steht dann eine Bewertung zu jeder bekannten Datei. Das Ergebnis wird lokal zwischengespeichert, sodass sich der Kommunikationsbedarf in Grenzen hält.

Im Vergleich zu einer klassischen Signaturprüfung benötigt der Agent auf den Endgeräten auf diese Art sehr viel weniger Ressourcen. Statt riesige Mengen von Mustern zu vergleichen und regelmäßig herunterzuladen, reicht eine Abfrage in der Cloud-Datenbank, die anders als eine Signaturliste enorm groß sein kann. Da sich Malware teilweise mehrmals am Tag ändert, ist so auch eine schnellere Reaktion möglich, als wenn jedes Mal erst eine Signatur erstellt und verteilt werden muss. Aber nicht nur Reputationen zu Dateien können mit so einem Mechanismus in einer Cloud-Datenbank abgefragt werden. Viele Produkte verarbeiten auf diesem Weg auch Reputationen zu IP-Adressen, Domänen oder URLs.

Weiter gehende Funktionen sind die Analyse von Metadaten verdächtiger Dateien in der Cloud oder sogar das Hochladen von Dateien, die dann in einer speziellen Sandbox-Analyseumgebung in der Cloud geöffnet und beobachtet werden. Die Ergebnisse solcher Analysen werden dann natürlich meist wieder in der Reputationsdatenbank gespeichert.

Mit künstlicher Intelligenz

Wie auch in anderen Bereichen der IT versuchen immer mehr Hersteller, Funktionen aus dem Bereich der künstlichen Intelligenz und des maschinellen Lernens für Malwareschutz anzuwenden. Die KI-Komponente kann dabei entweder in der Cloud des Herstellers oder auf dem Endgerät selbst liegen.

Die Aufgabe der KI ist meistens, Dateien als mutmaßlich gutartig oder bösartig zu klassifizieren. Firmen wie Cylance, DeepInstinct oder SparkCognition trainieren dafür in ihren Rechenzentren ein neuronales Netzwerk mit Millionen von bereits bekannten Malwaredateien und ebenso vielen gutartigen Dateien. Das Ergebnis ist ein neuronales Netz, das auch neue unbekannte Dateien mit einer sehr guten Trefferrate

Die Hersteller kurz vorgestellt

Avira

Avira ist ein deutscher Hersteller von Virenschutzprodukten. Die Firma wurde 1986 unter dem Namen H+B EDV gegründet und 2006 in Avira umbenannt. Firmensitz ist Tettnang am Bodensee. Das erste Produkt H+B AntiVir wurde 1988 veröffentlicht.

Bitdefender

Das Produkt von Bitdefender wurde ursprünglich im Jahr 1996 unter dem Namen AVX von der rumänischen Firma Softwin auf den Markt gebracht. 2001 entstand der Markenname Bitdefender, unter dem 2007 eine eigene Firma ausgegründet wurde. Das heutige Produkt wird unter dem Namen GravityZone vermarktet.

BlackBerry Cylance

Gegründet im Jahr 2012 von Stuart McClure (Ex-CTO McAfee) und Ryan Permeh (Ex-Chief Scientist McAfee) ist Cylance der vermutlich prominenteste Anbieter im Endpoint-Security-Markt mit Fokus auf künstlicher Intelligenz. Cylance versuchte von Anfang an, auf klassische Virenschutztechniken zu verzichten und stattdessen Dateien mithilfe eines neuronalen Netzwerks auf dem Endgerät zu klassifizieren. Im Jahr 2019 wurde Cylance vom Telefon- und MDM-Anbieter BlackBerry aufgekauft.

CarbonBlack (VMware)

CarbonBlack geht ursprünglich auf zwei Firmen zurück. Die 2002 gegründete Bit9 konzentrierte sich vor allem auf Application Whitelisting. Im Jahr 2014 kaufte Bit9 die 2010 gegründete Firma CarbonBlack, die sich auf Prozessverhaltensanalyse spezialisierte hatte. Das Unternehmen nannte sich danach bis 2016 „Bit9 + CarbonBlack". Im Jahr 2016 wurde mit Confer ein Hersteller einer Next-Generation-AV-Lösung dazugekauft und 2019 wurde CarbonBlack selbst von VMware übernommen – die ihrerseits genauso wie RSA zu EMC und damit zu Dell gehört.

Cisco

Cisco wurde 1984 von Wissenschaftlern der Stanford University gegründet und stellt primär Router und Switches her. 2013 übernahm Cisco die Firma Sourcefire, die mit dem Intrusion-Detection-System Snort bekannt geworden ist und auch ein Produkt zum Schutz vor Malware auf Endgeräten im Angebot hatte. Von diesem stammt das heutige AMP for Endpoints ab.

Bereits zehn Jahre früher (2003) hatte Cisco die Firma Okena mit ihrem Produkt StormWatch aufgekauft und so eines der ersten HIPS-Produkte (Host Intrusion Prevention System) in sein Portfolio aufgenommen. Aus StormWatch wurde danach der „Cisco Security Agent", den Cisco jedoch im Jahr 2010 abkündigte.

CrowdStrike

CrowdStrike wurde 2011 unter anderem von George Kurtz und Dmitri Alperovitch (ehemals McAfee) gegründet. Die ersten Produkte von CrowdStrike waren einerseits ein Threat-Intelligence-Service mit Hintergrundinformationen zu Angreifern, ihren Werkzeugen und Techniken und andererseits ein Produkt für Endpoint-Security, das zunächst seinen Fokus auf die Überwachung von Prozessen auf dem Endgerät richtete und dabei alle Informationen in der Cloud von CrowdStrike verarbeitete. Diese Lösung wurde unter anderem um proaktive Schutzfunktionen und Offlineschutz erweitert, hat aber immer noch einen Schwerpunkt auf der Erkennung und Reaktion (EDR) sowie dem Threat Hunting.

Cybereason

Cybereason ist ein Anbieter, der sich auf die Überwachung des Prozessverhaltens spezialisiert hat. Die Firma wurde 2012 in Israel gegründet. Als 2014 das erste Produkt auf den Markt kam, verlegten die Gründer das Headquarter nach Boston in die USA.

DriveLock

Die 1999 ursprünglich unter dem Namen CenterTools gegründete Firma hat ihren Sitz in München und ist vor allem für ihre Software im Bereich der Device-Kontrolle und Festplattenverschlüsselung bekannt. Virenschutz kam erst später hinzu. 2017 wurde der Firmenname in DriveLock geändert.

klassifizieren kann. Dieses trainierte Netzwerk wird dann den Kunden in Form eines Agenten zur Verfügung gestellt oder im Rahmen der Analyse von Dateien in der Cloud verwendet. Man kann es sich als mathematisches Modell vorstellen, das aus Eigenschaften von Dateien berechnet, ob eine Datei vermutlich schädlich ist.

Damit benötigt man keine Signaturen mehr und das ständige Aktualisieren von Signaturlisten kann entfallen. Das neuronale Netz selbst wird nur noch im Abstand von mehreren Monaten aktualisiert. Dadurch, dass diese KI auch unbekannte Malware erkennen kann, für die es noch keine Signaturen gibt, kommt ein solches System in Summe auf beeindruckende Erkennungsraten.

Natürlich hat aber auch diese Technik ihre Schattenseiten. In der Praxis verwenden die meisten Hersteller ihre KI-Komponente bisher nur zum Klassifizieren ausführbarer Programme. Für Office-Dokumente, Bilddateien oder PowerShell-Skripte ist sie meist nicht anwendbar, da man hierfür eigene Modelle mit anderen Eingangseigenschaften bräuchte. Auf Endgeräten, die sich bereits durch Application Whitelisting vor bösartigen Programmen schützen, ist der Mehrwert einer solchen KI-Komponente deshalb begrenzt, denn unbekannte Programme können ohnehin nicht ausgeführt werden.

KI: Segen, aber auch Fluch

Ein weiterer Nachteil besteht darin, dass man die KI umgehen oder auch angreifen kann. Ein professioneller Angreifer kann mit vertretbarem Aufwand seine Malware so gestalten oder umcodieren, dass die heute am Markt verfügbaren KI-Techniken sie nicht mehr erkennen können. Dann werden auch die langen Zeiträume zwischen den Updates des Modells zum Problem, denn mit Signaturen oder Reputationsabfragen kann eine solche Malware schnell blockiert werden, wenn sie dann doch einmal aufgefallen ist. Bis zum nächsten Update des KI-Agenten kann es aber Monate dauern, da der Vorgang des Trainierens eines neuronalen Netzwerks mit Millionen von Dateien so rechenaufwendig ist, dass der Hersteller hierfür viel Zeit benötigt.

Manche Hersteller verwenden die KI deshalb nicht als primären Erkennungsmechanismus im laufenden Betrieb, sondern im Backend, um neue Dateien im Rechenzentrum des Herstellers schnell zu bewerten und daraus dann automatisiert Signaturen oder Einträge in einer Reputationsdatenbank zu erstellen.

Ein ganz anderer Weg zum Schutz vor Malware ist die sogenannte Exploit Mitigation. Diese Technik versucht nicht, Malware vor ihrer Ausführung zu erkennen, sondern konzentriert sich darauf, das Ausnutzen von Softwareschwachstellen zu ver-

ESET

Die Geschichte der Firma ESET geht zurück auf Einzelpersonen, die schon Ende der 80er-Jahre Virenschutzsoftware in Bratislava in der ehemaligen Tschechoslowakei entwickelt haben. 1992 gründeten sie die Firma ESET und 1998 kam mit NOD32 ihre erste AV-Lösung für PCs auf den Markt. Die Firma ist nach wie vor im Privatbesitz und in Bratislava ansässig.

F-Secure

Die finnische Firma F-Secure wurde 1988 unter dem Namen Data Fellows gegründet und hat 1994 ihr erstes Virenschutzprodukt auf den Markt gebracht. 1999 wurde der Name in F-Secure geändert. F-Secure gehört damit zu den etablierten Herstellern von Virenschutz.

Fidelis Cybersecurity

Fidelis wurde 2002 gegründet und konzentrierte sich zunächst auf Netzwerk-Appliances mit Deep-Packet-Inspection-Features zur Erkennung von Datenabflüssen und Kompromittierungen im Netzwerk. 2012 wurde Fidelis an General Dynamics verkauft und 2015 von einer Investmentfirma wieder herausgekauft. Das Endpoint-Produkt basiert ursprünglich auf einer Lösung, die von Access Data für Incident Response entwickelt wurde. Dieser Geschäftsbereich wurde 2014 von Access Data als eigenständige Firma mit dem Namen Resolution1 herausgelöst und 2015 von Fidelis übernommen.

FireEye

Bereits 2004 gegründet, entwickelte FireEye zunächst ein Produkt zur Sandbox-Analyse. Es kam 2010 auf den Markt und erlaubte es, Dateien in einer gekapselten und überwachten Umgebung zu öffnen, um ihr Verhalten zu beobachtet und Schadcode zu erkennen. 2014 übernahm FireEye die Firma Mandiant, die zuvor vor allem als Anbieter für Incident Response und Forensik bekannt war und zu diesem Zweck auch eine Software entwickelt hatte. 2016 wurde die Firma iSIGHT Partners gekauft, ein Anbieter von Threat-Intelligence-Diensten.

G DATA

Bereits seit über 30 Jahren ist die deutsche Firma G DATA im Virenschutzmarkt aktiv. Sie wurde 1985 in Bochum gegründet und stellte 1987 das erste Virenschutzprodukt für den Atari-ST-Computer vor. G DATA gehört damit zu den ältesten Herstellern in diesem Markt.

HP (Bromium)

Gegründet wurde Bromium 2010 von Personen, die zuvor an der Universität Cambridge im Xen-Projekt intensiv mit Virtualisierungstechnik zu tun hatten. Der Hauptfirmensitz war zwar in den USA, das Entwicklungszentrum aber weiterhin in Cambridge, England. Das Produkt fällt in dieser Marktübersicht etwas aus dem Rahmen, da es fast ausschließlich auf Isolation durch Mikrovirtualisierung basiert. Inhalte, die aus nicht vertrauenswürdigen Quellen stammen, werden auf dem Endgerät immer durch einen Hypervisor isoliert geöffnet. Malware muss dabei nicht erkannt werden, denn sie kann aus ihrer Isolation nicht heraus und so auch keinen Schaden anrichten. Die typischen klassischen Funktionen einer AV-Lösung fehlen daher bei diesem Produkt. Im September 2019 wurde Bromium von HP übernommen.

itWatch

itWatch ist ein deutscher Anbieter mit Sitz in München. Die Firma wurde 2002 gegründet, wobei das erste Produkt schon vor der Firmengründung existierte. Bekannt geworden ist die Firma vor allem durch ihr Produkt zur Device-Kontrolle.

Ivanti

Ivanti und speziell ihre Sicherheitslösung für Endgeräte mit Fokus auf Application Whitelisting und Device-Kontrolle hat eine sehr bewegte Vergangenheit hinter sich. Die 1996 in Luxemburg gegründete Firma SecureWave hatte mit SecureExe als einer der ersten Anbieter ein Produkt zum Whitelisting erlaubter Programme entwickelt. Daneben hatte das Unternehmen ein Produkt zur Kontrolle von extern angeschlossenen Geräten unter dem Namen SecureNT. SecureWave schloss sich 2007 mit der Firma PatchLink zusammen, die vor allem für ihr Patch-

hindern. Durch zufällige Anordnung von Bereichen im Hauptspeicher, Markierung des Stacks als nicht ausführbar und viele weitere Techniken macht man es dem Angreifer schwer, seinen Exploit-Code erfolgreich zur Ausführung zu bringen. Viele dieser Techniken sind bereits Bestandteil moderner Betriebssysteme oder werden beim Kompilieren von Applikationen für das jeweilige Programm aktiviert. Einige müssen jedoch explizit für einzelne Programme konfiguriert und aktiviert werden. Schon unter Windows 7 gab es dafür das „Enhanced Mitigation Experience Toolkit“ (EMET), das Microsoft kostenlos zur Verfügung gestellt hat. Unter Windows 10 gibt es seit der Release 1709 den Windows Defender Exploit Guard und als Teil davon die Exploit Protection. Das Werkzeug ist nach wie vor kostenlos, muss aber vom Administrator konfiguriert werden.

Das ursprüngliche Produkt der Firma Cyvera, die 2014 von Palo Alto übernommen wurde, basierte in großen Teilen auf Exploit-Mitigation-Techniken. Palo Alto hat daraus das Produkt Traps gemacht und einige zusätzliche Funktionen eingebaut. Aber auch viele klassische AV-Hersteller haben Exploit-Mitigation-Funktionen in ihre modernen AV-Suiten integriert. Leider sind die Hersteller hier mit ihren Begriffen nicht immer eindeutig. Einige bieten Exploit-Protection-Funktionen, die nicht das Ausnutzen einer Schwachstelle erschweren, sondern danach Auffälligkeiten im Verhalten eines per Exploit manipulierten Prozesses erkennen und darauf reagieren.

Um Kompromittierungen von Endgeräten zu erkennen, ist in den letzten Jahren eine weitere neue Technik mit dem Namen Deception auf den Markt gekommen, die dem Angreifer Fallen stellt. Im Gegensatz zu klassischen Honeypots sind die Fallen dabei jedoch keine kompletten Systeme, sondern meist nur Fehlinformationen, die gezielt verteilt werden und für normale Anwender gar nicht sichtbar sind. Ein typisches Beispiel sind auf den Endgeräten gecachte administrative Credentials, die ein Angreifer mit Werkzeugen wie Mimikatz ausliest, um sie dann für einen Login auf anderen Systemen zu verwenden.

Deception: Dem Angreifer Fallen stellen

Ein Deception-Produkt würde unter anderem auf allen Arbeitsplätzen vorgetäuschte Credentials in diesen Speicherbereichen platzieren. Sobald ein Angreifer oder eine Malware diese ausliest und verwenden möchte, löst das Produkt Alarm aus. Besonders interessant an dieser Technik ist, dass sie in der Praxis so gut wie keine Fehlalarme erzeugt und damit der Betriebsaufwand minimal ist. Deception-Techniken sieht man am Markt vor allem bei spezialisierten Anbietern wie Illusive Networks

Die Hersteller kurz vorgestellt

Management-Produkt bekannt war. Dabei entstand der Name Lumension. Lumension schloss sich 2015 mit der Firma FrontRange zusammen und der Name wurde in HEAT Software geändert. 2017 kaufte der Besitzer von HEAT die Firma Landesk und verschmolz HEAT und Landesk zur heutigen Ivanti.

Kaspersky

Die Wurzeln des Virenschutzes von Kaspersky reichen zurück ins Jahr 1989, als Eugene Kaspersky als Hobby begann, sich mit Virenschutz zu beschäftigen und eine erste Software zu entwickeln. 1992 wurde sein Produkt unter dem Namen Antiviral Toolkit Pro von der Firma KAMI vermarktet. Die Firma Kaspersky Lab wurde dann im Jahr 1996 in Russland gegründet. Inzwischen gehört Kaspersky zu den weltweit größten Anbietern im Virenschutzmarkt.

McAfee

McAfee wurde 1987 von John McAfee gegründet und vermarktete sein Virenschutzprogramm ursprünglich als Shareware. Der Gründer zog sich nach dem Börsengang im Jahr 1994 aus dem Unternehmen zurück. 1997 schloss sich McAfee mit Network General als Network Associates (NAI) zusammen, trennte sich aber später wieder von deren Geschäftsbereich und änderte den Namen zurück auf McAfee. 2011 kaufe Intel die Firma McAfee, verkaufte jedoch 2017 wieder die Mehrheit an einen Investor. Das Produktportfolio von McAfee wandelte sich im Lauf der Jahre durch zahlreiche Firmenübernahmen. Dazu gehören beispielsweise SecureComputing und später Stonesoft im Firewall-Bereich, Reconnex und Onigma als DLP-Anbieter, Foundstone als Schwachstellenscanner, NitroSecurity im SIEM-Umfeld oder auch Dr. Solomons Group als Mitbewerber im Virenschutz.

Microsoft

Als Hersteller von Windows spielt Microsoft in dieser Marktübersicht eine besondere Rolle. Vor dem Erscheinen von Windows 10 wurde die Virenschutzlösung von Microsoft oft belächelt. Seit diese aber im Jahr 2017 massiv erweitert wurde, findet man den kostenlosen Microsoft Defender AV auch immer häufiger in Tests und Vergleichen von Virenschutzprodukten auf einem der vorderen Plätze. Dazu kommt, dass Windows 10 neben dem Defender AV viele weitere kostenlose Sicherheitsfunktionen wie AppLocker und Exploit Guard enthält. Erst der Defender ATP für das zentrale Management der Windows-Sicherheit und für die Überwachung des Prozessverhaltens ist für Unternehmen meist mit Mehrkosten verbunden, da er eine E5-Lizenz von Microsoft erfordert.

Panda Security

Panda Security ist ein weiterer europäischer Anbieter. Die Firma wurde 1990 in Spanien gegründet und bietet vor allem Sicherheitsprodukte für Endgeräte an.

Palo Alto Networks

Palo Alto Networks hatte zunächst wenig mit Endgerätesicherheit zu tun. Die Firma wurde im Jahr 2005 von Nir Zuk gegründet, der einer der ersten Firewall-Entwickler bei Checkpoint war, und konzentrierte sich ausschließlich auf Firewalls. Das Endpoint-Security-Produkt von Palo Alto wurde ursprünglich von der Firma Cyvera entwickelt und hat seinen Schwerpunkt im Bereich Exploit Mitigation. Cyvera wurde 2014 von Palo Alto übernommen.

RSA

Der Firmenname RSA Security stammt von den Initialen der Erfinder des RSA-Algorithmus Rivest, Shamir und Adleman ab, die im Jahr 1982 die Firma RSA Data Security grün-

oder CyberTrap, deren Produkte sich auf verschiedene Varianten von Deception konzentrieren. Aber auch einzelne Hersteller von AV-Suiten oder EDR-Produkten (Endpoint Detection and Response) haben Deception-Techniken integriert.

Ein Randbereich in dieser Marktübersicht sind Funktionen zum Schutz vor ungewolltem Datenabfluss. Die übliche Bezeichnung dafür ist DLP für Data Loss Prevention, Data Loss Protection oder auch Data Leakage Protection. In den Jahren 2000 bis 2007 gab es einige Start-ups und Nischenplayer, die eigene Produkte zum Erkennen und Verhindern von Datenabfluss entwickelt hatten. Hersteller wie Vontu, Onigma oder PortAuthority versuchten mit Sensoren im Mail-Gateway, im internen Netzwerk oder eben auf dem Endgerät zu erkennen, wenn Daten mit bestimmten Inhalten oder aus bestimmten Quellen versendet wurden. Im Jahr 2007 begannen dann etablierte AV-Hersteller solche Firmen aufzukaufen.

Weitere Mittel an Bord

Auf Unternehmens-Notebooks findet man neben einem Malwareschutz in der Regel auch eine VPN-Software für die sichere Kommunikation zwischen dem Notebook und dem Unternehmensnetz sowie eine Festplattenverschlüsselung zum Schutz der Daten und der Integrität des Betriebssystems. Festplattenverschlüsselung war früher einmal ein eigener Produktbereich mit spezialisierten Anbietern. Diese sind jedoch meist von größeren Anbietern aus dem AV- oder Firewall-Bereich aufgekauft und integriert worden. Für Unternehmen hat das den Vorteil, dass sie die Anzahl der Sicherheitsprodukte, die gleichzeitig auf den PCs der Mitarbeiter laufen müssen, reduzieren können.

Seit Microsoft mit BitLocker eine Festplattenverschlüsselungslösung bereits in Windows integriert hat, verschiebt sich der Markt weiter und viele Firmen verzichten zugunsten von BitLocker auf zusätzliche Festplattenverschlüsselungsprodukte, die eventuell in einzelnen Funktionsbereichen oder beim Managen überlegen wären.

Beim Malwareschutz ist eine ähnliche Tendenz erkennbar. Seit Microsoft im Jahr 2017 den in Windows 10 eingebauten Virenscanner (Defender AV) stark erweitert hat und mit Exploit Guard, Credential Guard und AppLocker zahlreiche Sicherheitsfeatures bereits kostenlos im Betriebssystem enthalten sind, ist der Markt stark in Bewegung.

Die Produktübersicht in der Tabelle

Die Marktübersicht enthält 27 Firmen, die Produkte im Bereich Endpoint-Security anbieten. Sie basiert auf der Auswertung von Fragebögen, die im Juli 2019 von der Redaktion an über 50 Hersteller versendet wurden. Ausgewählt wurden dafür Hersteller, die ein Produkt mit direktem Bezug zur Endgerätesicherheit von PCs anbieten. Leider haben nicht alle Hersteller an der Befragung teilgenommen, sodass einige Nischenplayer oder Spezialisten für Teilbereiche der Endpoint-Sicherheit nicht in der Übersicht enthalten sind. Die von den Herstellern zurückgesendeten Fragebögen wurden nach bestem Wissen und Gewissen ausgewertet und plausibilisiert, jedoch fanden keine Tests der Produkte statt.

Die so entstandene Feature-Matrix kann deshalb keine Aussage über die Qualität oder die erreichbare Schutzwirkung der Produkte machen. Man kann auch keinen „Gewinner“ daraus ableiten. Vielmehr soll sie einen Überblick über die relevanten

deten. Diese wurde im Jahr 1996 von der 1984 gegründeten Firma Security Dynamics aufgekauft, die vor allem für ihre SecurID-Tokens bekannt geworden war. 1999 änderte Security Dynamics seinen Namen in RSA Security, 2006 wurde RSA Security von EMC übernommen und 2016 kaufte Dell EMC, sodass RSA heute zu Dell gehört.

Der Einstieg in den Endpoint-Security-Markt begann für RSA im Jahr 2012 mit dem Aufkauf der Firma Silicium Security, die unter dem Namen ECAT ein Produkt zur Analyse von Endgeräten und Erkennung von Kompromittierungen entwickelt hatte. Dieses Produkt wurde mit der Netzwerkanalysetechnik von NetWitness zusammengeführt, die bereits 2011 von RSA übernommen wurde, und so wurde der Name ECAT in NetWitness Endpoint geändert.

SentinelOne

Die 2013 gegründete Firma SentinelOne hat wie viele Hersteller von Sicherheitsprodukten ihre Wurzeln in Israel und ihr Hauptquartier in den USA. Der Anbieter hat sich zunächst auf die Überwachung des Prozessverhaltens auf Endgeräten spezialisiert und erst später präventive Malwareschutzfunktionen hinzugefügt.

Sophos

Das britische Unternehmen Sophos wurde 1985 von zwei Entwicklern gegründet und brachte im Jahr 1988 das erste Virenschutzprodukt auf den Markt. Neben dem ursprünglichen AV-Bereich hat Sophos sein Portfolio durch einige Firmenzukäufe erweitert. Dazu gehörte unter anderem 2011 die deutsche Firma Astaro und 2017 Invincea, die Produkte im Bereich der Prozessverhaltensanalyse und der Isolation entwickelt hatte.

Symantec

Symantec wurde 1982 gegründet und war zunächst im Bereich künstliche Intelligenz (Sprachverarbeitung) und Datenbanken tätig. 1998 kam ein erstes AV-Produkt für den Macintosh auf den Markt. Nach der Übernahme der Peter Norton Computing kam 1991 ein Virenschutzprodukt für MS-DOS hinzu. 1991 wurden die Produkte dann als Norton Antivirus vermarktet. Für den Unternehmensmarkt wurde das Produkt später in Symantec Endpoint Protection umbenannt. Durch zahlreiche Firmenzukäufe hat sich Symantec zu einem der größten Anbieter im IT-Sicherheitsmarkt entwickelt. Zu den Zukäufen im Security-Umfeld gehörte beispielsweise Axent Technologies als Firewall-Hersteller, Security Focus als Pionier im Bereich Threat Intelligence, Brightmail als Anti-Spam-Lösung, PGP im Bereich Verschlüsselung oder BlueCoat Systems als Anbieter von Proxys. Im August 2019 wurde bekannt, dass Broadcom das Enterprise-Business von Symantec und damit auch die Endpoint-Security-Lösung übernehmen wird. Die Produkte für Endanwender sollen unter dem Norton-Label weiter vermarktet werden.

ThreatLocker

ThreatLocker ist der kleinste Anbieter dieser Marktübersicht. 2015 gegründet, konzentriert sich das Unternehmen auf Application Whitelisting und die Überwachung des Verhaltens von erlaubten Prozessen.

Trend Micro

Trend Micro wurde 1988 in Los Angeles als IT-Sicherheitsfirma gegründet und das Hauptquartier kurz darauf nach Taiwan verlegt. Nach der Übernahme durch eine japanische Firma wurde der Hauptsitz erneut verlegt, dieses Mal nach Tokio. Bereits 1990 erschien PC-cillin als Virenschutz für den Endverbrauchermarkt und kurz darauf auch als AV-Lösung für Unternehmen.

Hersteller und die von ihnen abgedeckten Funktionsbereiche geben. Für den individuellen Einsatz in Unternehmen kann es sinnvoll sein, einen Anbieter mit möglichst großer Abdeckung auszuwählen oder aber gezielt einzelne Spezialisten zu kombinieren, die in ihrem Bereich eventuell besser sind als ein Hersteller, der fast alles in einem Produkt abdeckt.

Funktionen wurden nur dann als „vorhanden“ gewertet, wenn der Hersteller diese Funktion in einem eigenen und verfügbaren Produkt anbietet. Features, die erst durch Integration von Drittprodukten anderer Hersteller ermöglicht werden oder die noch auf der Roadmap stehen, wurden als „nicht vorhanden“ gewertet. In vielen Fällen ist es zudem schwer, ein bestimmtes Feature klar als „vorhanden“ oder „nicht vorhanden“ zu bewerten, da Hersteller ihr eigenes Produkt gerne so positiv wie möglich darstellen und dabei durchaus kreative Argumente finden, warum ein bestimmtes Feature in ihrem Fall nicht nur gestreift wird, sondern tatsächlich vorhanden ist. Für die Matrix wurde deshalb versucht, Features nur als vorhanden darzustellen, wenn die Hersteller plausibel machen konnten, dass das jeweilige Feature auch die im Artikel beschriebenen Funktionen weitgehend abdeckt.

In der Übersicht findet man offensichtlich unterschiedliche Gruppen von Herstellern. Die größte Gruppe sind dabei die etablierten Hersteller aus dem Antivirus-Bereich wie McAfee, Symantec, Kaspersky, TrendMicro, F-Secure, G Data, ESET, Sophos oder Panda. Sie verkaufen in der Regel schon seit mehr als 20 Jahren Virenschutzprodukte und haben diese in den letzten Jahren stark erweitert. Sie decken so auch die neuen Funktionsbereiche ab, die zunächst nur von Nischenplayern angeboten wurden. Teilweise haben die Hersteller dafür solche Anbieter aufgekauft und sie in ihre Lösungen integriert.

Daneben gibt es die Firmen, die eher aus dem Netzwerk- oder Firewall-Bereich kommen, wie Cisco oder Palo Alto. Beide Firmen haben kleinere Sicherheitsfirmen aufgekauft, aus deren Produkten die heutigen Lösungen entstanden sind.

EDR – der neueste Hype

Noch eigenständige Spezialisten findet man vor allem mit Fokus auf EDR (Endpoint Discovery and Response). Darunter fallen beispielsweise FireEye, CrowdStrike, SentinelOne oder auch Cybereason. EDR ist dabei der aktuelle Hype im Bereich der Endpoint-Security. Im Wesentlichen konzentrieren sich diese Anbieter auf die bessere Erkennung kompromittierter Endgeräte und auf Features zur Analyse von Vorfällen, ihrer Eingrenzung und Reaktion darauf. Der tatsächliche Umfang der Detailfunktionen würde die Marktübersicht sprengen. Da der EDR-Markt zudem noch sehr jung und stark in Bewegung ist, wird dies ein Thema für eine zukünftige Marktübersicht.

Eine Sonderrolle in der Übersicht spielt offensichtlich Microsoft. Die Sicherheitsfunktionen, die Microsoft seit 2017 in Windows 10 eingebaut hat, sind umfangreich, überlappen sich an vielen Stellen mit den Features der klassischen AV-Hersteller, sind aber auch nicht alle kostenlos. Insbesondere der Defender ATP ist bisher nur in einer deutlich teureren E5-Lizenz zu haben. Insgesamt sorgt das Engagement von Microsoft auf jeden Fall für einige Bewegung im Markt. (ur@ix.de)

Stefan Strobel

ist Buchautor sowie Gründer und Geschäftsführer des IT-Sicherheitshauses cirosec.