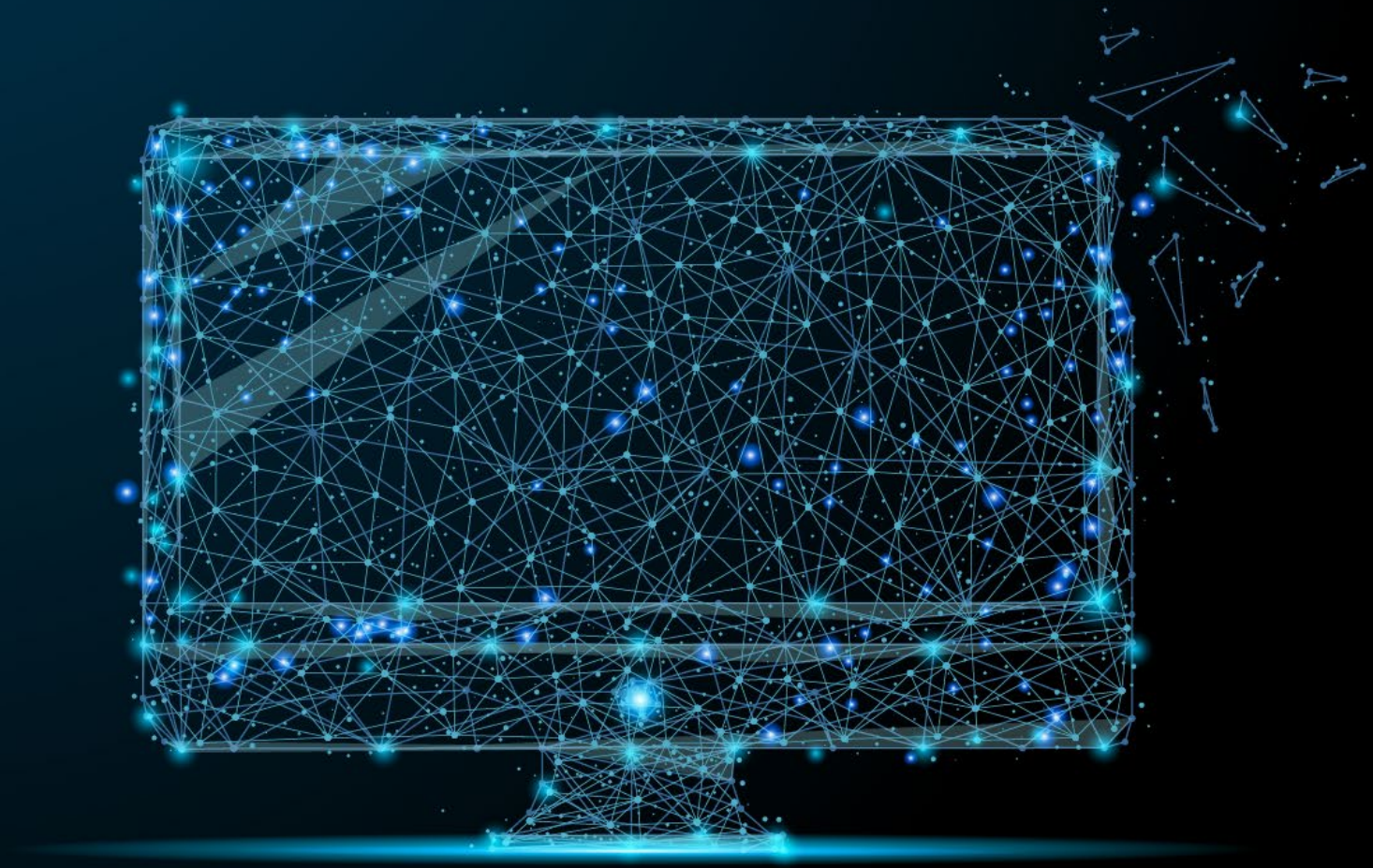
VMRAY

RÖNTGENBLICK FÜR MALWARE



Mit modernen Methoden moderner Malware entgegentreten

Die Abwehr bislang unbekannter Malware stellt viele IT-Security-Teams vor Probleme. Nun steht eine neue Technologie bereit, um auch modernste Angriffe automatisiert und trotzdem präzise zu analysieren und erfolgreich zu bekämpfen.

Die Zeiten, in denen ein vergleichsweise simpler Virenscanner und eine Firewall genügten, um ein Unternehmen vor Cyber-Angreifern zu schützen, sind lange vorbei. Im Laufe der Jahre haben Kriminelle immer neue Tricks entwickelt, um in fremde Netze einzudringen, Daten zu stehlen und teils erheblichen Schaden anzurichten. Singuläre Sicherheitsmaßnahmen reichen nicht mehr aus, um dieser Bedrohung zu begegnen.

Im Idealfall verfügt ein Unternehmen über ein engmaschiges System aus mehreren Sicherheitsmaßnahmen, das Malware zuverlässig erkennt und stoppt. Neben Antivirus und Firewall setzen Unternehmen heute IDS-/IPS-Lösungen (Intrusion Detection und Prevention Systems) zur Erkennung und Abwehr von Angriffen ein, ebenso E-Mail- und Web-Gateways zum Filtern des ein- und ausgehenden Traffics. Eine immer größere Rolle spielt zudem die Segmentierung des Netzwerks, um einem an einer Stelle erfolgreichen Eindringling den Zugriff auf weitere Teile der IT-Umgebung zu verwehren.

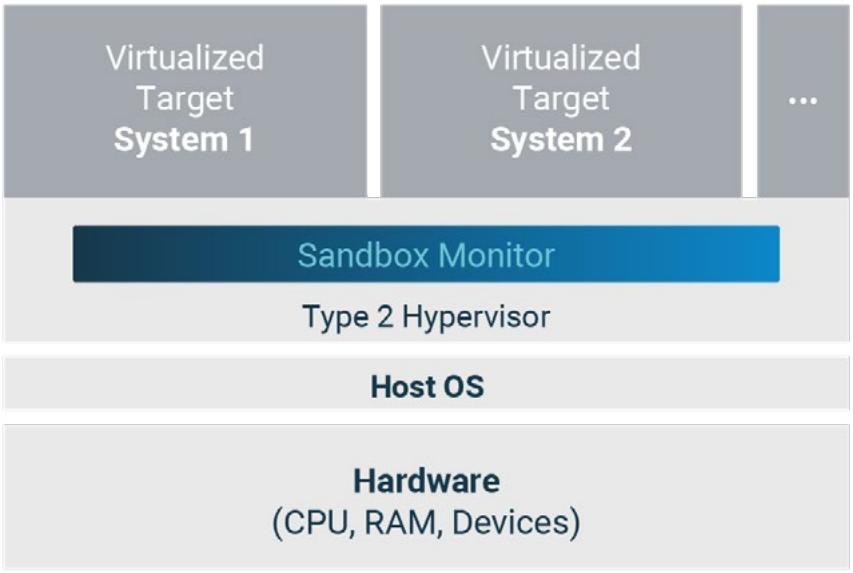
Eine große Lücke bestand aber bislang bei der Erkennung und Abwehr sogenannter evasiver Malware, bei Zero-Day-Attacken und bei gezielten Angriffen gegen Unternehmen und Führungspersonen.

INHALTSVERZEICHNIS

Schon seit über zehn Jahren experimentieren Sicherheits-forscher daher in diesem Bereich mit verhaltensbasierter Erkennung auf Basis von Sandboxen: Eine klassische, zur Malware-Analyse eingesetzte Sandbox ähnelt einer voll-ständigen Betriebsumgebung, wie sie der Schädling nor-malerweise antreffen würde. In dieser Umgebung kann die Malware kontrolliert gestartet und in ihrem „normalen“ Ver-halten beobachtet werden. Das unterscheidet dieses Ver-fahren von statischen Analysen, bei denen eine verdächtige Datei nur anhand bestimmter fixer Merkmale und Hash-Werte
geprüft wird. Obwohl statische Analysen sehr gut skalier-bar sind, lassen sie sich doch relativ leicht umgehen, indem die Schädlinge zum Beispiel minimal verändert werden.

Zunächst war die Sandbox-Methode sehr erfolgreich. Doch den Cyber-Gangstern blieb auch diese Weiterentwicklung auf Dauer nicht unbekannt. Sie passten ihre Schädlinge so an, dass sie sich in einer virtuellen Umgebung sofort de-aktivieren. Frische Denkansätze waren also nötig, um den Kampf gegen neue Malware nicht zu verlieren. Nur dann lassen sich auch „Advanced Threats“ erkennen und erfolg-reich abwehren. Anders als frühe Sandboxen mussten die neuen Methoden hochautomatisiert, präzise und bestens skalierbar sein, so dass selbst in großen Umgebungen kei-ne Performance-Probleme auftreten.

Wie innovative Sandboxen die Malware-Erkennung verbessern



Wenn das Monitoring im Hypervisor statt in der virtuellen Maschinen stattfindet, kann eine Malware nicht mehr herausfinden, ob sie beobachtet wird oder nicht.

Herkömmliche Techniken zur dynamischen Malware-Analyse in einer virtuellen Umgebung basieren meist auf einer vollständigen System-Emulation. Dabei werden entweder die Hardware oder das Betriebssystem nachgebildet. Diese Methode ist jedoch in der Regel sehr aufwendig, komplex und zudem kostspielig. Außerdem lassen sich diese Lösungen nur schlecht skalieren, so dass es zu unvollständigen oder ungenauen Ergebnissen kommt. Und: Es gibt mehrere Möglichkeiten für eine Malware, diese Formen der Emulation zu erkennen und sich dann abzuschalten. Das trifft ganz besonders auf die OS-Emulation zu, die daher kaum noch eingesetzt wird.

Eine erste Weiterentwicklung besteht im „Hooking“. Dabei wird kein emuliertes, sondern ein echtes System eingesetzt. Anfragen an dieses System werden über „Hooks“ umgeleitet. Allerdings kann eine Malware auch diese Technik leicht erkennen. Zudem entstehen relativ schnell Performance-Probleme, wenn zu viele Anfragen in kurzer Zeit abgefangen werden müssen. Es bedurfte also einer Lösung, bei der eine Malware nicht mehr merkt, dass sie in einer Sandbox beobachtet wird. Genau hier setzt ein auf dem Hypervisor basierender Ansatz an, mit dem sich die Aktivitäten in der Ziel-Maschine komplett von außerhalb der Analyse-Umgebung überwachen lassen. Selbst hoch entwickelte evasive Malware kann dann nicht mehr erkennen, dass sie eigentlich in einem isolierten Käfig läuft und unter genauer Beobachtung steht.

VMRAY

Tipps für die Wahl einer Sicherheitslösung

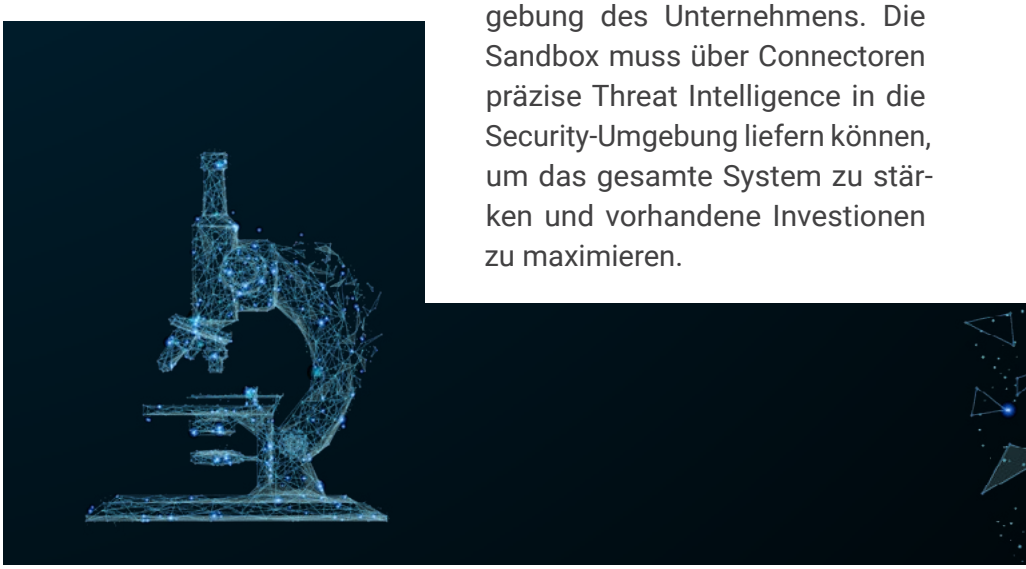
Die folgenden Punkte sind entscheidend, wenn es um eine geeignete Analyse-Plattform geht:

1 **Skalierbarkeit:** Eine effektive Analyse ist nur möglich, wenn die eingesetzten Maßnahmen automatisiert und je nach Bedarf skaliert werden können. Die Ergebnisse müssen dabei immer zuverlässig und vollständig bleiben.

2 **Schutz vor evasiven Maßnahmen:** Traditionelle Sicherheitslösungen befinden sich in einem fortdauernden Rüstungswettlauf mit den Cyber-Kriminellen, der auf Dauer nicht zu gewinnen ist. Zu den wichtigsten Schutzmaßnahmen gehört daher, eine Analyse-Plattform zu nutzen, die von der Malware nicht erkannt und vermieden werden kann.

3 **Vorhandene Systeme stärken:** Wichtig ist die Integration in die bestehende Security-Umgebung des Unternehmens. Die Sandbox muss über Connectoren präzise Threat Intelligence in die Security-Umgebung liefern können, um das gesamte System zu stärken und vorhandene Investionen zu maximieren.

4 **Risikoeinschätzungen und Scoring:** Selbst die beste Analyse-Plattform überlastet die firmeneigenen Sicherheitsteams, wenn sie nicht über automatisch erstellte Risikoeinschätzungen und ein solides Scoring verfügt. Nur damit lassen sich Gefahren zuverlässig einordnen und schneller angemessene Maßnahmen ergreifen.



Der Hypervisor ist die Schicht, auf der die virtuellen Maschinen mit den Sandbox-Umgebungen laufen. Während der Analyse wird die Aktivität in der Sandbox mithilfe von Virtual Machine Introspection (VMI) komplett von außerhalb der VM überwacht. Die Vorgehensweise wird durch Intermodular Transition Monitoring (ITM) ergänzt. Dank dieser Methode wird kein Monitoring-Agent mehr innerhalb der Kapsel benötigt, der von einer Malware erkannt werden könnte. Von der neuen Technik profitieren private Unternehmen, kritische Infrastrukturen und Regierungsbehörden, die Sandboxing einsetzen können, um moderne Malware abzuwehren. Es ist wichtig, dass eine Beobachtung nicht erkannt wird, da eine verseuchte Datei ansonsten im schlimmsten Fall als sauber eingestuft und für die Ausführung freigegeben wird.

VMRAY

WAS ES SONST NOCH ZU BEACHTEN GILT:

Anders als bei den früheren Ansätzen ist das Monitoring jetzt also direkt in den Hypervisor eingebettet. Mit Hilfe von „Golden Images“ lässt sich mittlerweile die echte IT-Umgebung eines Unternehmens täuschend ähnlich nachbilden. Damit können Sicherheitsexperten auch die – aus guten Gründen – besonders gefürchteten gezielten Angriffe erkennen, die nur auf Rechnern der ins Visier genommenen Organisation aktiv werden. Heute ist es auch kein Problem mehr, per Geo-Location festzulegen, in welchem Land sich ein simulierter Rechner befinden soll. Die Sicherheitsteams in den Unternehmen können dadurch beobachten, wie sich ein Cyber-Angriff entwickelt und welche Aktionen die Schadsoftware ausführt. Mit Hilfe einer automatisch erstellten Bewertung ergreifen sie dann geeignete Gegenmaßnahmen, die eine Beeinträchtigung der echten IT-Umgebung verhindern.

Ein weiterer Vorteil der innovativen Methode besteht darin, dass dank der präzisen, rauschfreien Analyse-Reports auch die Fehlarlarme zurückgehen. Jeder erfahrene Cyber Threat Analyst weiß, dass nach einer gewissen Zeit eine „Alert Fatigue“ auftritt. Dann wird es immer schwerer, echte von falsch erkannten Angriffen (False Positives) zu unterscheiden. Desweiteren können automatisch generierte Indicators of Compromise (IOC) an andere Security-Systeme bereitgestellt werden, um z.B. Blockierungen von Endpoints und andere Sicherheitsmaßnahmen auszulösen.

Prozessautomatisierung bei der Malware-Erkennung und -Analyse sind weitere wichtige Vorteile in Zeiten von Fachkräftemangel und dünner Personaldecke. Automatisierte Erkennungsprozesse sind skalierbar, sodass auch Teams mit geringer Personalstärke den stetigen Anstieg im Malwareaufkommen bewältigen können. Moderne Sandboxing-Lösungen zwingen die Schädlinge, sich zu enttarnen und decken zugleich wesentliche Informationen über neue Angriffsvektoren auf. Dadurch lassen sich Lücken in der Verteidigung schließen, der Schutz im Unternehmen erhöht sich deutlich.

HYPERVISOR-BASIERTE PLATTFORM ZUR MALWARE-ANALYSE UND ERKENNUNG

Der Bochumer Security-Spezialist VMRay hat einen einzigartigen Ansatz entwickelt, um auch hoch entwickelte Malware zu erkennen und abzuwehren. Die Plattform besteht aus einer mehrstufigen Sicherheitsarchitektur, die für eine zuverlässige Erkennung von Bedrohungen sorgt.

Im ersten Schritt wird eine auf Reputation beruhende Malware-Analyse durchgeführt, anschließend eine statische Untersuchung und zuletzt eine dynamische Analyse in einer Hypervisor-basierten Sandbox. Möglich sind zudem eine erweiterte Web-Analyse zur Erkennung von Phishing-Angriffen sowie von Drive-By-Downloads, und seit kurzem auch eine Prüfung von verdächtigen Links.

Last not least: VMRay nutzt mehrere nach ISO 27001 zertifizierte und GDPR-Standards entsprechende Rechenzentren in Deutschland und den USA. Daher lassen sich mit der Plattform sowohl die Vorgaben der europäischen Datenschutz-Grundverordnung (DSGVO), als auch die des California Data Privacy Act sowie der Singapore Monetary Authority Guidelines einhalten.