SCHÜTZEN SIE IHRE DATEN

OPTIMALE ERKENNUNG VON CYBER BEDROHUNGEN FÜR UNTERNEHMEN

TABIDUS
TECHNOLOGY
UNITED MALWARE PROTECTION

www.tabidus.com

INHALT

1 DIE GEFAHREN DER DIGITALEN WELT

WAS MACHT DIE DIGITALE WELT SO GEFÄHRLICH – VOR ALLEM FÜR UNTERNEHMEN?

Der Betrieb eines jeden modernen Unternehmens ist von einer funktionierenden IT-Infrastruktur abhängig. Dazu gehört natürlich auch die Cyberwelt in all ihren Formen. Obwohl die digitale Revolution eine Unmenge von Vorteilen mit sich brachte, lauern auch viele Gefahren unter der Oberfläche, die jedem Unternehmen bewusst sein müssen. Neben der allgegenwärtigen Bedrohung durch Netzangriffe ist Malware eine der größten Gefahren für die IT-Infrastruktur und die Daten eines Unternehmens.

WAS IST MALWARE?

Malware ist eine Art von Software, die Schäden an Clients, Servern oder Netzwerken verursachen kann, sobald sie in ein System eingeschleust wurde. Es gibt viele verschiedene Arten von Cyber- Bedrohungen, die unter dem Oberbegriff „Malware“ zusammengefasst werden. Jede von diesen führt ihren Angriff auf unterschiedlichen Wegen, zu verschiedenen Zwecken und mit individuellen Effekten aus. Im Folgenden werfen wir einen Blick auf die verbreitetsten Arten von Malware, für die ein Unternehmen anfällig sein kann.

1. ADWARE

AdWare steht als Abkürzung für „Advertising-Supported Software“, im Deutschen also so viel wie „werbegestützte Software“. Häufig wird AdWare-Malware mit der bösartigeren „Spyware“ kombiniert, die Benutzeraktivitäten verfolgt und – weit schlimmer noch - Informationen von dem jeweiligen System entwendet. AdWare selbst stiehlt Speicherplatz auf einem Endgerät und kann es verlangsamen. In der Regel fungiert diese Malware aber als umsatzgenerierendes Werkzeug für Werbetreibende und wird häufig mit dem Download von Software und Apps in Form von „kostenlosen Versionen“ verbreitet.

2. BOTS

Der Zweck eines Bots ist die Automatisierung von Vorgängen auf einem Gerät. Diese Art von Malware ist in den letzten Jahren immer gefährlicher geworden. Ganze „Botnetze“ werden beispielsweise von Cyberkriminellen eingesetzt, um eine Vielzahl an Rechnern kontrollieren zu können. Bots werden unter anderem für DDoS-Angriffe (Distributed Denial of Service), als Webspider zum Abgreifen von Serverdaten, als Spambots, die Werbung auf Webseiten platzieren, sowie zur Verbreitung von Malware über Download-Portale eingesetzt.

3. BUGS

Bugs sind Softwarefehler die für gewöhnlich durch menschlichen Irrtum beim Schreiben des Quellcodes oder durch Compiler entstehen können. Grundsätzlich ist ein Bug einfach ein Fehler, der zu einem unerwünschten Ergebnis führt. Kleinere Bugs können lange Zeit unentdeckt bleiben, da ihre Auswirkung auf das Verhalten des jeweiligen Programms relativ gering sind. Leider sind jedoch nicht alle Fehler so problemlos. Schwerwiegendere Bugs können dazu führen, dass ein Gerät einfriert oder gar abstürzt. Die schwerwiegendsten Fehler sind Sicherheitslücken, die es Angreifern ermöglichen können, Zugriffsrechte zu überschreiben, die Benutzerauthentifizierung zu umgehen und Daten zu stehlen.

4. RANSOMWARE

Diese Art von Malware schränkt den Zugriff auf den Computer ein, indem sie entweder Dateien auf der Festplatte verschlüsselt oder das System komplett sperrt. Im letzteren Fall wird dann eine Nachricht angezeigt, die den Benutzer auffordert, ein „Lösegeld“ an den Malware-Ersteller zu bezahlen, um die Einschränkungen aufzuheben. Ransomware wird in der Regel über einen Datei-Download oder eine andere Art von Schwachstelle in einem Netzwerk verbreitet.

5. ROOTKIT

Diese Form von Malware ist darauf ausgelegt, Cyberkriminellen einen Fernzugriff zu ermöglichen oder die Kontrolle über ein Gerät zu übernehmen, ohne dabei von Sicherheitssoftware erkannt zu werden. Da ein Rootkit extrem gut darin ist, sich der Erkennung zu entziehen, kann es sehr schwierig sein, einen solchen Befall zu verhindern oder das Rootkit zu entfernen – sofern man es denn überhaupt entdeckt!

6. SPYWARE

Spyware überwacht die Benutzeraktivität, zeichnet Tastatureingaben auf und sammelt Daten (wie zum Beispiel Kontoinformationen, Login- und Finanzdaten). Häufig ist Spyware auch dazu in der Lage, die Sicherheitseinstellungen von Anwendungen oder Browsern auf dem Gerät zu ändern und die Netzwerkverbindungen zu beeinträchtigen. Spyware nutzt Schwachstellen im Netzwerk aus und versteckt sich oft in legitimer Software oder in Trojanern.

7. TROJANER

Ein Trojaner tritt in Gestalt eines normalen Programms oder einer regulären Datei auf, verleitet den Benutzer dann aber, ihn herunterzuladen und zu installieren. Der Angreifer hinter dem Trojaner erhält dann Zugriff auf das befallene Gerät, so dass er zum Beispiel Daten stehlen (einschließlich Login-Daten bis hin zu sensiblen Bank-Informationen), Dateien ändern, Benutzeraktivitäten überwachen, den Computer innerhalb von Botnetzen nutzen und weitere Malware installieren kann.

8. VIRUS

Ein Virus ist in der Lage, sich selbst zu kopieren und zu verbreiten. Er ist ansteckend und verteilt sich automatisch auf andere Computer, indem er sich an Programme anhängt und Code ausführt, wenn ein Anwender auf das infizierte Programm zugreift. Neben Programmen werden Viren häufig auch über Skriptdateien und Dokumente sowie über Webanwendungen verbreitet, wobei Sicherheitslücken durch Cross-Site-Scripting (XSS) ausgenutzt werden.

9. WÜRMER

Würmer verbreiten sich über Netzwerke, durch Ausnutzung von Schwachstellen im Betriebssystem, verbrauchen Bandbreite und überlasten Server. Diese Schadprogramme werden meist durch E-Mails mit infizierten Anhängen verbreitet und können sich selbstständig replizieren und ausbreiten.

Malware wird häufig entwickelt und verbreitet, um die größtmögliche Anzahl von Geräten auf der ganzen Welt zu erreichen und eine Vielzahl von Zielen zu attackieren. Obwohl viele Ziele wahllos ins Visier geraten, existieren auch Angriffe, die auf ein ganz bestimmtes Unternehmen ausgerichtet sind und einen sehr speziellen Zweck erfüllen. Meist findet Malware den Weg in ein Unternehmen über Kanäle wie E-Mails, Downloads aus dem Internet oder über ein infiziertes mobiles Gerät bzw. Datenspeicher.

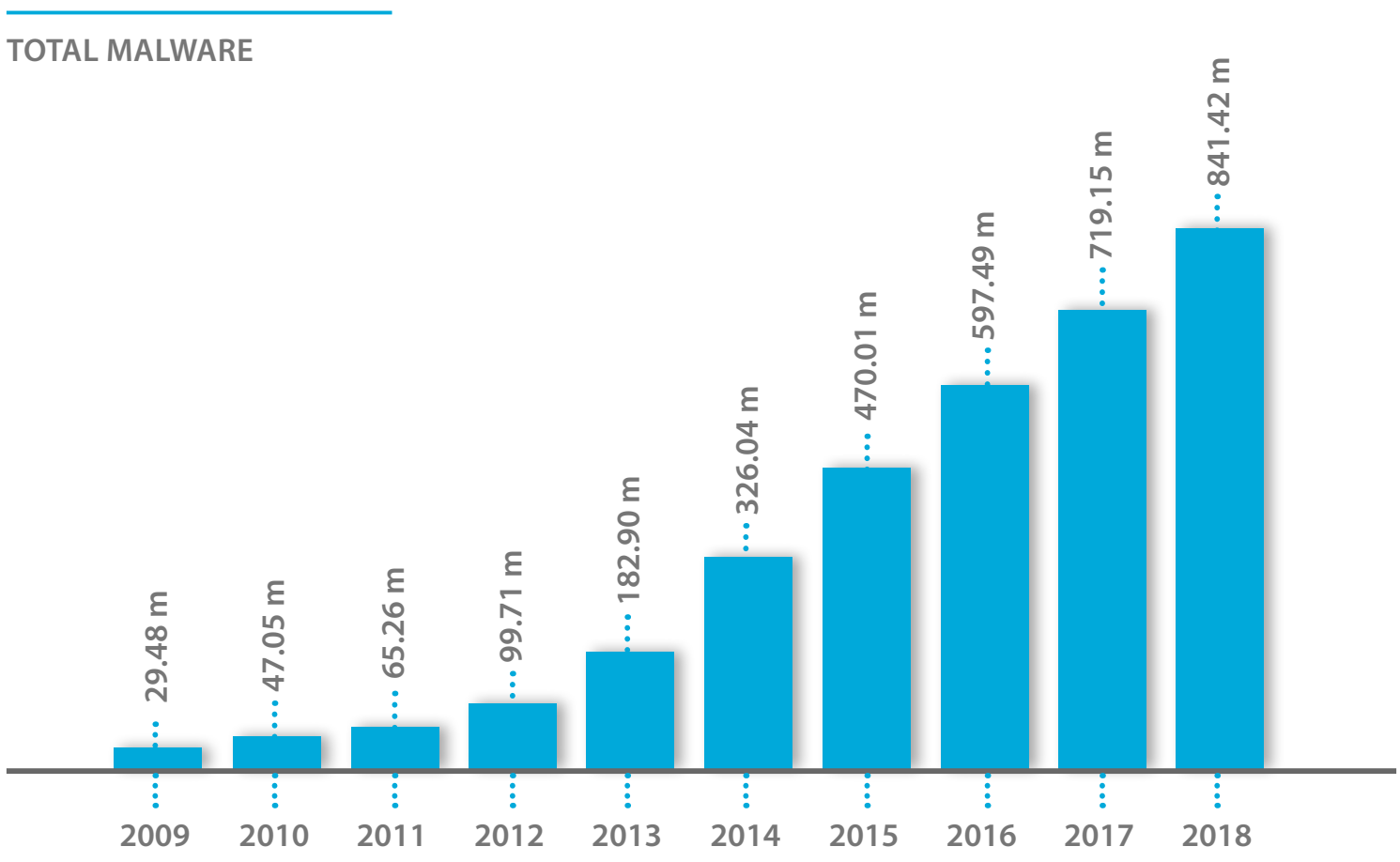
Nach Angaben des Instituts AV-Test werden täglich über 350.000 neue Schadprogramme registriert und die Zahl steigt jedes Jahr. Im Jahre 2009 wurden beispielsweise „nur“ 29,48 Millionen Malware und PUA (potenziell unerwünschte Anwendungen) identifiziert. Im Jahr 2018 lag diese Zahl bereits bei 841,42 Millionen.

DIE FRAGE NACH DEM WARUM

Die große Frage ist: Was ist verantwortlich für diesen rapiden Zuwachs an Malware? Ein Blick auf die Angreifer selbst und deren Motivation kann dies beantworten...

„SCRIPTKIDDIES“

Inzwischen kommt es immer häufiger vor, dass Malware-Angriffe von Nicht-Profis ausgeführt werden, die über keine speziellen Fähigkeiten verfügen. Diese sogenannten „Scriptkiddies“ nutzen Skripte oder Programme, um Schwachstellen in Geräten oder Systemen auszunutzen, die bereits von anderen entdeckt und kommuniziert



Source : www.av-test.org

wurden, meist im „Dark Web". In der Regel geht es diesen Angreifern nur um den reinen Nervenkitzel. Sie greifen oft nach dem reinen Zufallsprinzip an, ohne überhaupt genau zu verstehen, welche Auswirkungen ihre Handlungen haben können. Ein gutes Beispiel für einen solchen Scriptkiddie-Angriff ist der TalkTalk-Hack von 2015, in dessen Zuge die britische Datenschutzbehörde ICO eine Rekordstrafe für den Telekommunikationsanbieter verhängte und der das Unternehmen 42 Millionen Pfund kostete. Die Person hinter dem Angriff? Ein 17-jähriger Jugendlicher, der zugab, dass die Attacke nur dazu diente, um anzugeben.

HACKTIVISMUS

Sogenannte „Hacktivisten" greifen aus ideologischen oder politischen Gründen an und nehmen dabei bestimmte Unternehmen oder Institutionen ins Visier, um Medienaufmerksamkeit und öffentliches Interesse an ihrer Sache zu erzeugen. Sie sind in der Regel nicht finanziell motiviert, sondern zielen darauf ab, umstrittene Angelegenheiten und vermeintliche Korruption aufzudecken. Ein gutes Beispiel ist der Skandal um die „Panama Papers" von 2016. Das Ziel des Angriffs, der sich gegen die panamaische Anwaltskanzlei Mossack Fonseca richtete und in dessen Rahmen etwa 11,5 Millionen Dokumente aufgedeckt wurden, war es, die Offshoring-Aktivitäten einer Reihe von hochrangigen Persönlichkeiten ans Tageslicht zu bringen.

ORGANISIERTE KRIMINALITÄT

Motiviert durch finanziellen Gewinn agieren organisierte kriminelle Vereinigungen, um sensible Finanzdaten zu erhalten oder die Kontrolle über Zahlungssysteme zu gewinnen. Sie können Ransomware verwenden (etwa beim DD4bC-Angriff im Jahr 2015) oder es darauf anlegen, Zugang zu sensiblen oder vertraulichen Daten zum Zwecke der Erpressung zu erhalten (zum Beispiel beim Angriff auf die Europäische Zentralbank 2014).

NATIONALSTAATEN ODER STAATSNAHE ORGANISATIONEN

Staatlich gesteuerte Cyberangriffe (oder solche von staatsnahen Organisationen), die zu politischen Zwecken begangen werden, stehen heute mehr denn je im Rampenlicht. Ein Grund dafür ist, dass Russland vorgeworfen wird, an der Manipulation der US-Wahlen im Jahr 2016 beteiligt gewesen zu sein. Obwohl die Details solcher Angriffe streng geheim bleiben, scheinen die Beweggründe in der Störung von militärischen Operationen, der politischen Stabilität und kritischen Infrastrukturen zu liegen.

INSIDER

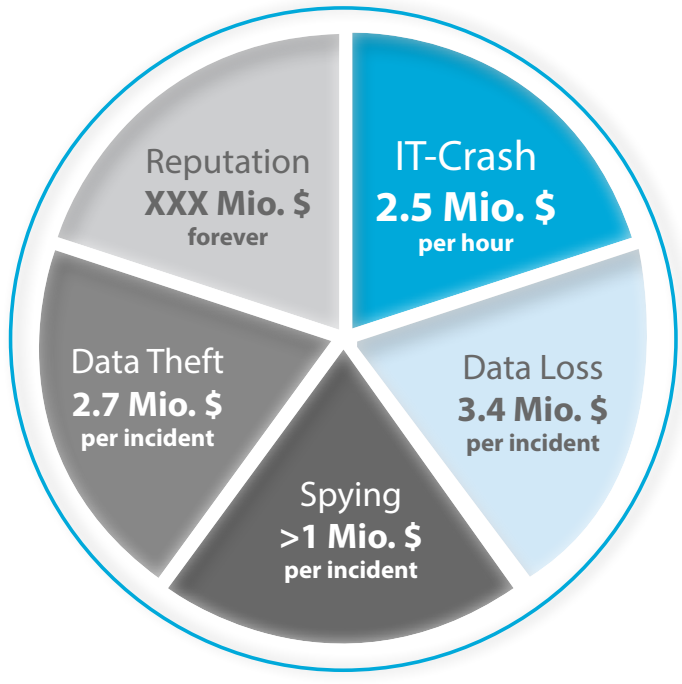
Beunruhigenderweise können auch verärgerte Mitarbeiter (sowohl ehemalige als auch aktuelle) hinter Angriffen auf Unternehmen stehen. Motiviert durch „Rachegefühle" oder aus purer Bosheit können Insider-Angriffe darauf abzielen, geistiges Eigentum oder Daten zu stehlen oder sogar die Systeme des Unternehmens grundlegend zu beschädigen. Morgan Stanley wurde im Jahr 2015 Opfer eines solchen Insiderangriffs, als ein Mitarbeiter angeblich 730.000 Kundendaten aus dem System löschte.

DIE KONSEQUENZEN FÜR UNTERNEHMEN

Ein einziges Malware Exemplar kann wirtschaftliche Schäden in astronomischer Höhe verursachen, wenn dieses nicht richtig erkannt und unschädlich gemacht wird. Der Schaden für ein Unternehmen kann dabei auf vielfältige Weise spürbar sein, von den unmittelbar sichtbaren Folgen (Computerabstürze und Produktionsausfälle) bis hin zu den besonders heimtückischen und zunächst unsichtbaren Konsequenzen, die sich oft erst lange Zeit später bemerkbar machen . Die Auswirkungen eines Angriffs werden noch schlimmer, wenn auch Kunden, Partner und die Öffentlichkeit darauf aufmerksam werden. Die negativen Folgen eines solchen Reputationsverlustes können die finanziellen Kosten sogar noch weit übersteigen.

Darüber hinaus können rechtliche Konsequenzen entstehen. IT-Leiter und Geschäftsführer können in der persönlichen Haftung für den Angriff stehen – mit Folgen, die von Bußgeldern (einschließlich Entschädigungszahlungen) bis hin zu Freiheitsstrafen wegen Fahrlässigkeit reichen. Das Unternehmen kann von Datenschutzbehörden überprüft werden und Ansprüche wegen Urheberrechtsverletzungen und Verletzungen geistigen Eigentums können ins Spiel kommen. Auch negative Ratings von Banken und Investoren können die Folge sein. Versicherungen werden möglicherweise ungültig oder sind nicht mehr zu vernünftigen Konditionen abschließbar. Im schlimmsten Fall kann dem Unternehmen sogar die Gewerbeerlaubnis entzogen werden. Zumindest muss aber davon ausgegangen werden, dass die für den Vorfall verantwortlichen Personen zurücktreten müssen oder entlassen werden.

WIRTSCHAFTLICHER SCHADEN



Source: Contingency Planning and Management

2 MÖGLICHE **SICHERHEITSMASSNAHMEN**

WAS KÖNNEN UNTERNEHMEN TUN, UM SICH VOR BEDROHUNGEN ZU SCHÜTZEN UND SCHÄDEN ZU VERMEIDEN?

Um Malware-Vorfälle und deren Folgen zu vermeiden, bietet die IT-Sicherheitsbranche ein breites Spektrum an Lösungen und Maßnahmen. Diese lassen sich grundsätzlich in drei Kategorien unterteilen:

PRÄVENTIVE MASSNAHMEN

Die erste Möglichkeit, zu der ein Unternehmen greifen kann, ist die Einführung von Präventivmaßnahmen. Das Ziel ist dabei, die Angriffsfläche zu reduzieren. Dazu muss das Unternehmen jedoch einige wesentliche Einschränkungen für den Umgang mit Firmengeräten erlassen. Beispiele für solche vorbeugenden Maßnahmen sind:

- Einsatz einer Firewall, um ausschließlich autorisierten Netzwerkverkehr zuzulassen
- Sperrung des Internetzugangs oder Verwendung eines URL-Filters, um bestimmte Arten von Webseiten zu blockieren
- Sperrung des Empfangs bestimmter Dateitypen (wie.exe- und. zip-Dateien) per E-Mail oder Download
- Einsatz einer Kennwortrichtlinie und von Authentifizierungssystemen (wie Smartcards, Biometrie oder Zwei-Faktor-Authentifizierung)
- Einführung eines Whitelist-Ansatzes, bei dem ausschließlich vordefinierte Programme ausgeführt werden können
- Blockierung oder Begrenzung der Verwendung von Wechseldatenträgern
- Suche nach möglichen Angriffsvektoren (Vulnerability Detection) und Patchen der Systeme

SICHERHEITSBEWUSSTSEIN SCHAFFEN

Die zweite Möglichkeit ist die Schulung und Sensibilisierung der Mitarbeiter für den sicheren Umgang mit IT und Daten. Viele Mitarbeiter haben keine Kenntnisse über Internetsicherheit und die damit verbundenen Gefahren. Es ist deshalb eine gute Idee, Mitarbeiter zu schulen, damit sie die Risiken verstehen und wissen, was zu tun ist, um die Angriffsfläche nach Möglichkeit zu minimieren. Solche Schulungen könnten zum Beispiel folgende Aspekte umfassen:

- Öffnen Sie keine dubiosen E-Mails von Ihnen unbekannten Absendern
- Sprechen Sie nicht mit Außenstehenden über firmeninterne Einzelheiten und verwendete Systeme
- Schließen Sie weder Ihren privaten USB-Stick noch einen fremden Stick an einen Firmenrechner an
- Bringen Sie keinerlei elektronische Gadgets und Geschenke mit zur Arbeit und verwenden Sie diese auch nicht auf Geräten, mit denen Sie auf Unternehmensdaten zugreifen
- Verwenden Sie komplexe Passwörter und variieren Sie diese zwischen verschiedenen Plattformen

ERKENNUNG VON BEDROHUNGEN

Die dritte Möglichkeit besteht darin, direkt Jagd auf Bedrohungen zu machen und festzustellen, was „gut" und was „böse" ist. Wenn sich das Unternehmen in der glücklichen Lage befindet, eigene Malware-Analysten zu beschäftigen, ist das hervorragend. Alle anderen müssen sich hingegen an einen Sicherheitsanbieter wenden, der ihnen die Analyse und Erkennung von Bedrohungen in Form einer technischen Lösung, wie beispielsweise eines Antivirenprogramms, anbietet. Es stehen bereits hunderte solcher Sicherheitsprodukte von einer Vielzahl an Anbietern zur Auswahl, mit unterschiedlichsten Ansätzen zur Erkennung von Bedrohungen.

Signaturbasiert

Eine Signatur beschreibt eine bekannte Bedrohung, identifiziert eine Datei oder einen Registry Key sowie alle zugehörigen Teile einer Bedrohung und definiert deren Bösartigkeit (z.B. auf Basis des HASH-Wertes). Derartige Signaturen werden von großen Expertenteams durch die Analyse von zur Verfügung stehenden Beispielen erstellt. Über ein „Signatur-Update" werden diese für den automatisierten Download in entsprechenden Produkten bereitgestellt.

Heuristik-basiert

Heuristisches Scannen bewertet die Code- und Verhaltensmuster einer Datei oder eines ausführenden Prozesses hinsichtlich deren Ähnlichkeit mit bekannten Malware-Typen. Wenn festgestellt wird, dass eine Datei bzw. ein Prozess Muster enthält oder Aktivitäten ausführt, die mit bekannten Bedrohungen übereinstimmen, wird davon ausgegangen, dass diese „böse" ist. Heuristisch basiertes Scannen ist insofern effektiv, als dass es das Potenzial besitzt, zukünftige Bedrohungen bereits zu erkennen, ohne dass die Malware im Vorfeld erkannt, übermittelt, analysiert und mit einer Signatur ausgestattet werden muss.

Cloud-basiert

„Cloud" bezieht sich in diesem Kontext auf ein oder mehrere Rechenzentren eines IT-Security- Anbieters, mit denen sich Geräte und Anwendungen jederzeit verbinden und Daten abrufen können. Bei dieser Form des Malware-Scannens findet die Prüfung nicht direkt am Endgerät statt, sondern wird an den Anbieter ausgelagert. In der Regel tritt ein Verdachtsmoment auf dem lokalen Computer auf,

woraufhin die Datei oder ihr HASH-Wert zur weiteren Überprüfung an den Sicherheitsanbieter übermittelt wird. Anschließend wird ein Bericht über die Einstufung der Datei und eventuelle Intentionen retourniert. Mit der Cloud-basierten Methode stehen Informationen schneller zur Verfügung als beispielsweise über Signaturen und es können mehr Überprüfungen stattfinden, als auf einem lokalen Gerät.

Sandboxing

Der Sandbox-Ansatz zielt darauf ab, anhand eines Verhaltens zu erkennen, ob etwas „gut" oder „böse" ist. Dies funktioniert zwar nicht mit jedem Dateityp, aber bei ausführbaren Dateien (zum Beispiel.exe- oder .dll-Dateien) zeigt dies Wirkung. In der Regel wird die betreffende Datei in eine virtuelle, sichere Umgebung übertragen und dort ausgeführt. Das Verhalten in dieser Umgebung wird anschließend auf bestimmte Aktionen hin überwacht, die für Malware typisch sind (zum Beispiel, ob eine Verbindung zu einer Internetadresse aufgebaut, neue Dateien erstellt oder Verschlüsselungsversuche unternommen werden). Diese Beobachtungen entscheiden dann darüber, ob eine Einstufung als „gut" oder „böse" erfolgt.

Intrusion Detection

Dieser Ansatz versucht nicht direkt Malware zu erkennen, sondern vielmehr, ob ein bereits bekannter Angriffsweg ausgenutzt wird. In der Regel werden dazu API-Aufrufe auf dem Betriebssystem überwacht und wenn diese mit einem bekannten Angriff oder einer bekannten Schwachstelle übereinstimmen, wird der Zugriff blockiert oder ein Alarm ausgelöst. In manchen Fällen wird auch das normale Verhalten einer Anwendung vordefiniert und Gegenmaßnahmen eingeleitet, sobald diese davon abweicht.

Maschinelles Lernen

Beim maschinellen Lernen soll die Technologie auf der Grundlage früherer Erfahrungen selbstständig darüber entscheiden, was „gut" und was „böse" ist. Während der Ausführung eines Programms wird dessen Verhalten überwacht und mit bestehenden Daten verglichen. Wenn das gezeigte Verhalten dem bereits vorhandenen Wissen ähnelt, wird davon ausgegangen, dass auch das Ergebnis vergleichbar ist. Eine völlig neuartige Ransomware zeigt zum Beispiel ein ähnliches Verhalten wie bereits bekannte Varianten (etwa die Verschlüsselung von Systemdateien) und daher behandelt das maschinelle Lernsystem dieses neue Exemplar wie dessen Vorgänger.

3 WELCHE MASSNAHMEN FUNKTIONIEREN IN DER PRAXIS?

Trotz der vielen möglichen Maßnahmen und verfügbaren Lösungen in der Branche ist IT-Sicherheit nach wie vor eine große Herausforderung für Unternehmen. Dies gilt vor allem, weil ein Kompromiss zwischen Sicherheit und Produktivität gefunden werden muss. Im Folgenden werfen wir daher einen genaueren Blick auf die Praxistauglichkeit der vorgestellten Maßnahmen.

WELCHE DER VORGESCHLAGENEN MASSNAHMEN KÖNNEN DURCHGEFÜHRT WERDEN UND WELCHEN SCHUTZ BIETEN SIE?

PRÄVENTIVE MASSNAHMEN

Die Ergreifung von vorbeugenden Maßnahmen kann ein Unternehmen vor vielen bekannten und unbekannten Bedrohungen schützen. Für viele Unternehmen sind derartige Maßnahmen in der Praxis jedoch äußerst schwer umzusetzen, denn diese bedeuten in der Regel große Einschränkungen der Produktivität der IT-Systeme. Benötigte oder wichtige Funktionalitäten sind dadurch standardmäßig verboten oder blockiert, wodurch das Unternehmen gezwungen ist entsprechende Ausnahmen einzurichten, um die Produktivität aufrecht zu erhalten. Folglich entsteht ein administrativer Alptraum für die IT-Abteilung, gepaart mit spürbaren Unannehmlichkeiten für die Mitarbeiter. Zudem können zwar viele Bedrohungen mit präventiven Maßnahmen verhindert werden, aber vollständige Sicherheit wird dadurch nicht erzielt. Selbst die für eine einwandfreie Funktionalität erforderlichen Ausnahmeregelungen sind im Endeffekt wieder neue Sicherheitslücken.

Fazit: Vorbeugende Maßnahmen können ein guter Ausgangspunkt sein, soweit ein Unternehmen diese in der Praxis umsetzen kann. Als alleinige Sicherheitsstrategie ist Prävention jedoch nicht ausreichend.

SICHERHEITSBEWUSSTSEIN

Mitarbeiter darin zu schulen, beim Umgang mit Passwörtern, Informationen, Endgeräten, Links, E- Mails usw. vorsichtiger zu agieren, kann hilfreich sein und möglicherweise dazu beitragen, einige gefährliche Situationen zu vermeiden. Allerdings handelt es sich hierbei nur um eine partielle Lösung. Menschen machen zwangsläufig Fehler. Ebenso ist die Geräte- und Netzwerksicherheit für die einzelnen Mitarbeiter in der Praxis häufig von geringerer Priorität, da nicht ihre eigenen Daten oder Geräte gefährdet sind. Viele Bedrohungen sind außerdem selbst für sensibilisierte Mitarbeiter nur schwer zu erkennen. Spam-E-Mails zum Beispiel sind heutzutage oft so gut gemacht, dass es selbst Experten schwerfällt, diese ohne technische Unterstützung zu identifizieren.

Fazit: Schulung und Sensibilisierung der Mitarbeiter sind wichtige Aspekte, die aber keine funktionale Lösung darstellen.

ERKENNUNG VON BEDROHUNGEN

Das direkte Erkennen, Jagen und Blockieren von Bedrohungen mit Hilfe von Technologien, die von IT- Sicherheitsanbietern bereitgestellt werden, zählt für die meisten Unternehmen zu den bevorzugten Sicherheitsstrategien. Jedes Unternehmen kann solche Lösungen installieren, sie schaffen direkte Sicherheit und blockieren ausschließlich die „bösen Dinge". Theoretisch sollte die Erkennung von Bedrohungen durch technologische Mittel daher die ideale Herangehensweise sein. Aber der Fall gestaltet sich deutlich komplexer, als den meisten Unternehmen bewusst ist. Es gibt eine ganze Reihe von Fragen, die sich ein Unternehmen stellen muss, wenn es sich mit einer Strategie zur Erkennung von Bedrohungen beschäftigt:

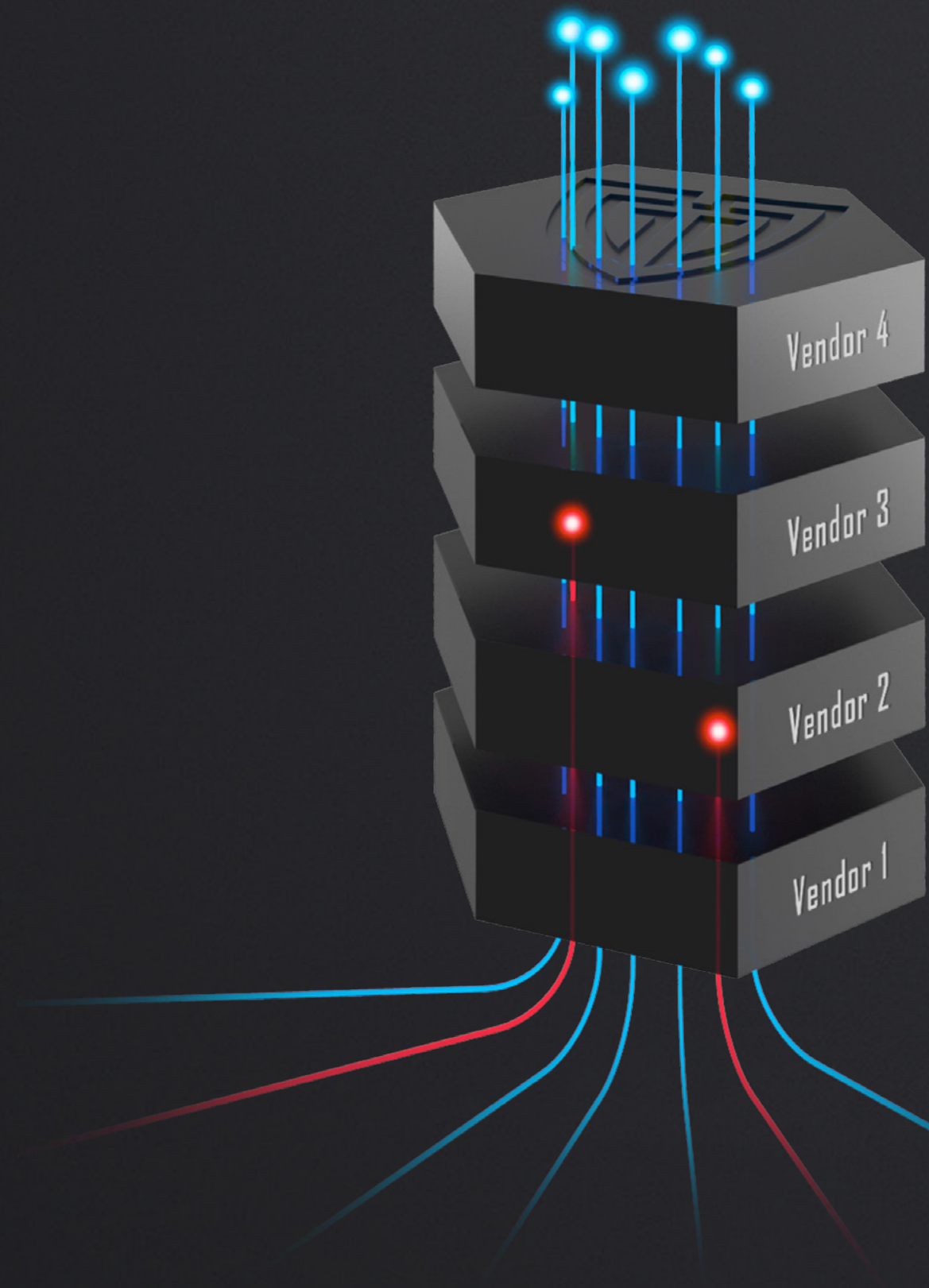
- Welche Lösung soll ich einsetzen?
- Nach welchen Kriterien soll ich diese auswählen?
- Welcher technologische Ansatz ist der beste?
- Welcher Anbieter bietet den besten Schutz?
- Wem soll ich vertrauen?

Aufgrund von technischen Einschränkungen muss in der Regel ein einzelner Anbieter ausgewählt oder es müssen miteinander kompatible Lösungen gefunden werden. Nachdem die erste strategische Entscheidung getroffen wurde, beginnt ein langwieriger Implementierungs- und Schulungsprozess, um die Lösung betreiben zu können. Und was passiert danach? Entgegen weit verbreiteter Annahmen ist kein Sicherheitsprodukt eines einzelnen Anbieters in der Lage, 100- prozentigen Schutz zu bieten – ungeachtet vom eingesetzten Ansatz. Zu den häufigsten Problemen, die bei der Erkennung von Bedrohungen durch einzelne Sicherheitslösungen auftreten, zählen unter anderem:

- False-Negatives: Kein Anbieter kann alles erkennen; einige Bedrohungen schlüpfen immer durch das Netz
- False-Positives: Manchmal werden legitime Dateien fälschlicherweise als bösartig eingestuft, was fatal sein kann
- Reaktionszeiten können zu lange sein, wodurch Bedrohungen erst zu spät erkannt werden
- Die Beseitigung einer Bedrohung erfolgt nicht immer vollständig
- Technische Störungen wie Performance-Probleme treten auf
- Mehrere Lösungen müssen eingesetzt werden, um alle Bereiche abzudecken

Fazit: Im Vergleich zu Präventivmaßnahmen und Steigerung des Sicherheitsbewusstseins ist die Bedrohungserkennung für die meisten Unternehmen einfacher umzusetzen, da nur „die bösen Dinge" blockiert werden und der bezahlte Sicherheitsanbieter sich darum kümmert. Aber die korrekte und rechtzeitige Erkennung aller weltweiten Bedrohungen ist für einen einzelnen Anbieter nahezu unmöglich. Folglich kommt es weiterhin zu Sicherheitsvorfällen, trotz investierter Zeit und Geld für die Installation einer Sicherheitslösung.

AGILE **ERKENNUNG VON BEDROHUNGEN**



4 AGILE STRATEGIE ZUR ERKENNUNG VON BEDROHUNGEN

Wie kann ein Unternehmen eine zufriedenstellende Bedrohungserkennung erreichen und Malware- Vorfälle so gut wie möglich vermeiden, ohne die typischen Probleme und Einschränkungen in Kauf nehmen zu müssen? Am Anfang steht eine einfache Entscheidung...

SOLLEN WIR UNS FÜR EINEN EINZELNEN HERSTELLER ODER FÜR EINEN VERBAND VON HERSTELLERN ENTSCHEIDEN?

Anstatt einen einzelnen Hersteller auszuwählen und dessen Lösung zu implementieren, können Sie sich für einen Verband von Herstellern wie Tabidus Technology entscheiden.

Ein Verband von Herstellern unterscheidet sich grundlegend von einzelnen IT-Sicherheitsprodukten. Anstatt eine oder mehrere einzelne Lösungen zu installieren, wird ein universelles Sicherheits-Framework (beispielsweise der United Endpoint Protector) installiert, dass die Technologien mehrerer Anbieter beherbergt. Das Framework ermöglicht eine flexible Aktivierung und Kombination der verschiedenen Technologien per Mausklick, zu jeder Zeit, passend zu jedem Bedürfnis. Der Verband sorgt dabei für eine reibungslose Zusammenarbeit der einzelnen Anbieter innerhalb des Sicherheits-Frameworks.

Diese Flexibilität verändert den Umgang mit Sicherheitsanbietern und bildet die Grundlage für eine agile Strategie zur Erkennung von Bedrohungen. Dieser Ansatz hat eine ganze Reihe von positiven Auswirkungen auf die Qualität der Bedrohungserkennung:

ERKENNUNGSRATE

Die Fähigkeit, „gut" von „böse" zu unterscheiden, differiert von Fall zu Fall und von Hersteller zu Hersteller. Prinzipiell hängt alles vom aktuellen Wissensstand und dem technologischen Ansatz des jeweiligen Anbieters ab. Durch die Möglichkeit, voneinander unabhängige Hersteller zu kombinieren, können Lücken bei der Erkennung von Bedrohungen geschlossen werden.

FALSE-POSITIVES HANDHABUNG

Fehlalarme sind ein ernsthaftes Problem bei der Erkennung von Bedrohungen. Der Einsatz mehrerer unabhängiger Hersteller mit unterschiedlichen Ansätzen für individuelle Probleme kann dazu beitragen, die negative Auswirkungen in solchen Fällen zu vermeiden. Eine Datei soll zum Beispiel erst dann gelöscht werden, wenn mindestens zwei unterschiedliche Anbieter sie als bösartig eingestuft haben.

REAKTIONSZEIT

Ein wichtiger Aspekt bei der Erkennung von Bedrohungen ist die rechtzeitige Verfügbarkeit des Wissens über die Bedrohung. Dies ist besonders dann relevant, wenn der technologische Ansatz Aktualisierungen (Signaturen) benötigt oder der Anbieter Anpassungen vornehmen muss, um eine bestimmte Bedrohung zu erkennen. Der Einsatz mehrerer unabhängiger Anbieter kann sicherstellen, dass das erforderliche Wissen in der kürzest möglichen Zeit durch den jeweils schnellsten Hersteller verfügbar ist.

Der Einsatz einer agilen Erkennungsstrategie verbessert nicht nur die Qualität der Bedrohungserkennung, sondern hat darüber hinaus auch weitere positive Auswirkungen auf den Betrieb.

FREIHEIT ZU WÄHLEN

Anstatt einen einzelnen Sicherheitsanbieter zu evaluieren und auszuwählen, dem das Unternehmen folglich vertrauen muss, können mehrere Hersteller gleichzeitig ausgewählt werden. In diesem Fall ist die Evaluierung vergleichsweise einfach, da die gewünschte Technologie per Klick aktiviert wird und sofort zur Verfügung steht. Welche Hersteller, wie viele Hersteller, mit welchem Ansatz und welchen Technologien ausgewählt werden, liegt ganz in den Händen des Unternehmens selbst.

INDIVIDUELLE ANFORDERUNGEN

Eine moderne IT-Infrastruktur besteht aus verschiedenen Bereichen mit jeweils eigenen Anforderungen an das Sicherheitssystem. Mit einem einzelnen Sicherheitsprodukt kann es schwierig sein, all diesen individuellen Anforderungen zu entsprechen. Eine agile Strategie ermöglicht es hingegen, Anbieter passend zu jedem Einsatzgebiet zu aktivieren und zu kombinieren. Dadurch wird gewährleistet, dass in jedem Anwendungsfall der jeweils optimale Technologiemix zum Einsatz kommt.

HOT SWAP

Herkömmliche IT-Sicherheitslösungen müssen fix installiert werden, was einen späteren Austausch zu einem aufwendigen und langwierigen Vorgang macht. Mit einem universellen Sicherheits-Framework werden Anbieter und deren Technologien nicht fest installiert, sondern einfach per Mausklick aktiviert. Änderungen können damit sehr einfach, ohne erneuten Software-Rollout, im laufenden Betrieb, innerhalb weniger Minuten und auf Wunsch unternehmensweit durchgeführt werden. Das Unternehmen kann daher jederzeit seine Entscheidungen ändern. Anbieter können nach Belieben aktiviert und deaktiviert werden, und ein neuer Hersteller mit einem neuen Ansatz lässt sich mit wenigen Klicks einbinden.

EINHEITLICHE LÖSUNG

Aus verschiedenen Gründen können innerhalb eines Unternehmens bereits mehrere Sicherheitslösungen betrieben werden. Diese Form einer „Multi-Vendor-Strategie" bedeutet, dass jede Lösung separat betrieben und gewartet werden muss, was einen großen Aufwand mit sich bringt. Innerhalb eines universellen Sicherheits-Frameworks kommen zwar mehrere Anbieter zum Einsatz, dennoch handelt es sich immer noch um eine einzige Lösung. Alles ist in einer einheitlichen Benutzeroberfläche vereint und die Betriebs- und Wartungskosten entsprechen denen einer herkömmlichen Einzellösung.

STRATEGIEN

Der Einsatz eines universellen Sicherheits-Frameworks kann sich auch auf die Sicherheitsstrategien auswirken. Durch die Möglichkeit von Hot-Swap-Änderungen, Multi-Vendor-Nutzung und einer freien Anbieterauswahl stehen zusätzliche Kriterien für strategische Entscheidungen zur Verfügung. Die Gestaltung der Strategie nach Anbieter, Einsatzbereich, Sicherheitsfunktion und zeitlicher Verwendung ermöglicht gänzlich neue Ansätze. Etwa zeitgesteuerte Kontrollinstanzen mit zusätzlichen Technologien oder einen permanenten Einsatz mehrerer Anbieter, um nur einige Beispiele zu nennen.

SICHERHEITSVORFALL

Wie kann auf einen Sicherheitsvorfall reagiert werden, der von der eingesetzten Sicherheitslösung nicht erkannt oder bekämpft wird? Bei traditionellen Ansätzen, in denen ein fixer Sicherheitsanbieter zum Einsatz kommt, ist ein solches Szenario häufig der Beginn einer langen Tortur. Oft endet diese mit dem Download eines Säuberungs-Tools eines Drittanbieters, das auf einen USB-Stick kopiert und zur manuellen Bereinigung jedes einzelnen Rechners verwendet werden muss. Eine agile Sicherheitsstrategie ermöglicht hingegen die einfache Aktivierung eines zusätzlichen Anbieters, der die erforderliche Erkennungsrate besitzt und sich innerhalb weniger Minuten – netzwerkweit – um den Vorfall kümmert.

COMPLIANCE

Verschiedene Gesetzesnormen, wie zum Beispiel die ISO 27001, verlangen von Unternehmen den Einsatz von Multi-Vendor-Strategien. Die Installation mehrerer separater Sicherheitslösungen stellt zwar den Gesetzgeber zufrieden, führt aber zu einem großen Mehraufwand für das Unternehmen. Das Sicherheitsniveau wird dadurch auch nicht signifikant erhöht, da weiterhin nur jeweils ein einzelner Anbieter aktiv ist. Ein universelles Sicherheits-Framework kann eine gute Alternative für Unternehmen sein, um gesetzliche Anforderungen zu erfüllen und gleichzeitig die Sicherheit nachhaltig zu verbessern.

5 MYTHEN UND **FAKTEN**

In der Vergangenheit gab es bereits Multi-Engine-Lösungen, die nicht immer gute Arbeit geleistet haben, und vielerorts ist zu lesen, dass die gleichzeitige Installation mehrerer Antivirenlösungen keine gute Idee ist. Es entstand eine Gerüchteküche mit vielen Vorurteilen, die auch nicht immer sachlich begründet sind. Im Folgenden wollen wir Licht ins Dunkel bringen.

„DIE KOMBINATION MEHRERER IT-SICHERHEITSPRODUKTE IST KEINE GUTE IDEE“

Das ist wahr... wenn von eigenständigen Sicherheitslösungen gesprochen wird. Einzelne Lösungen sind meist nicht dafür konzipiert, um mit anderen Lösungen zusammenzuarbeiten. Ein spezielles Sicherheits-Framework ist erforderlich, damit mehrere Anbieter reibungslos zusammenarbeiten können. Tabidus kombiniert keine Sicherheitsprodukte, sondern den jeweiligen Technologiekern der einzelnen Hersteller, um eine gute Performance zu erzielen.

„MEHRERE SICHERHEITSPRODUKTE BIETEN KEINEN BESSEREN SCHUTZ“

Jeder IT-Sicherheitsanbieter verfügt über sein individuelles Wissen und seine eigenen Technologien zur Erkennung von Bedrohungen, was zu einem individuellen Schutzpotential führt. Dieses wird laufend von neutralen Institutionen wie AV-Test oder AV-Comparative getestet. Kein einziger Anbieter kann immer jede mögliche Bedrohung erkennen, aber der intelligente und zielgerichtete Einsatz mehrerer Anbieter erhöht den Erkennungsgrad, stellt eine vollständige Entfernung der Bedrohung sicher und verkürzt gleichzeitig die Reaktionszeiten. Damit kann sichergestellt werden, dass Bedrohungen rechtzeitig erkannt und beseitigt werden.

„MEHRERE SICHERHEITSPRODUKTE SIND EIN PERFORMANCE-KILLER“

Eine gleichzeitige Verwendung herkömmlicher Sicherheitsprodukte führt in der Tat zu erheblichen Performance-Problemen.
Die Kombination von Kerntechnologien, die reibungslos zusammenarbeiten, ist hingegen etwas ganz anderes. Die Performance hängt lediglich davon ab, wie schnell jede einzelne Komponente ist und wie diese eingesetzt wird.

Der flexible Einsatz von Technologien und Herstellern ermöglicht Unternehmen, die Kombinationen für jede Sicherheitsfunktion getrennt festzulegen. Mit dieser Methode können beispielsweise Technologien mit einem hohen Datendurchsatz für Echtzeit-Anwendungen und andere für zeitgesteuerte Scans ausgewählt werden. Damit kann immer der optimale Mix aus Technologien für jedes Einsatzgebiet erzielt werden, ohne jegliche Performance-Probleme.

„DER BETRIEB MEHRERER SICHERHEITSLÖSUNGEN ERZEUGT GROSSEN MEHRAUFWAND“

Wenn viele Einzellösungen gleichzeitig betrieben werden, entsteht dadurch tatsächlich ein großer Mehraufwand – ungeachtet der Performance-Probleme, die ein solcher Ansatz erzeugen kann!
Alle Wartungsarbeiten, Überwachungen etc. müssen mehrfach durchgeführt werden. Bei Tabidus wird hingegen alles zu einer einzigen Lösung zusammengeführt. Trotz dem Einsatz von mehreren Sicherheitsanbietern muss nur eine einzige Lösung betrieben werden.

„ES SIND BEREITS MEHRERE SICHERHEITSANBIETER IM EINSATZ“

Ja, es stehen viele eigenständige Sicherheitslösungen zur Auswahl, die verschiedenste Aspekte der Cybersicherheit abdecken können. Gelegentlich werden diese in Form von Pseudo-Multi-Vendor-Strategien betrieben, bei denen sich beispielsweise eine Lösung um den Schutz der Serverlandschaft und eine andere um die der Clients kümmert.

In diesen Fällen entsteht jedoch ein großer Mehraufwand und eigenständige Lösungen sind in Betrieb. Mit Tabidus können mehrere Anbieter gleichzeitig auf demselben System und ohne zusätzlichen Aufwand betrieben werden, um die wahre Leistungsfähigkeit einer echten Multi- Vendor-Strategie voll auszuschöpfen.

„ES EXISTIEREN BEREITS MULTI-ENGINE LÖSUNGEN“

Multi-Engine-Lösungen sind grundsätzlich in drei verschiedenen Kategorien verfügbar:

1. ONLINE-SCANNER (WEBSEITEN)

Es existieren mehrere Webseiten, auf denen Dateien manuell hochgeladen werden können, um dann eine Antwort zu erhalten, welcher Sicherheitsanbieter eine Erkennung durchführen würde. Diese Portale sind eher als Nachschlagewerke und nicht als Sicherheitslösungen zu verstehen.

2. WEB UND EMAIL

Im Bereich der Web- und E-Mail-Sicherheitslösungen werden manchmal Multi-Engine-Lösungen eingesetzt. Diese schützen jedoch nur den Web- und E-Mail-Verkehr, jedoch nicht die vollständigen Endgeräte. In den meisten Fällen existiert dabei auch keinerlei Flexibilität.

3. KOOPERATION VON ANBIETERN

Bei manchen IT-Sicherheitslösungen ist eine zweite oder dritte Engine verfügbar. Diese ist jedoch meist im Hintergrund versteckt und fest verankert, ohne jegliche Flexibilität. Der Grund für den Einsatz weiterer Engines ist meist eine Kooperation zwischen Anbietern, wenn der ursprüngliche Anbieter nicht genügend Bedrohungen abdecken kann und „hinter den Kulissen" Unterstützung benötigt.

Alles diese Arten von Multi-Engine-Lösungen haben eines gemeinsam: Sie bieten nicht die Flexibilität und das Endpoint-Sicherheitsniveau von Tabidus.

„ANTIVIRUS IST TOT"

Es ist wichtig, zu verstehen, was genau mit dem Begriff „Antivirus" gemeint ist.

„Antivirus" im Sinne von „Endgeräteschutz" ist und wird immer ein wichtiger Bestandteil einer jeden Sicherheitsstrategie sein. Abhängig vom Angriffsweg und der Art der Bedrohung ist der Endgeräteschutz die erste und zugleich letzte Verteidigungslinie.

„Antivirus" im Sinne von „signaturbasierter" Erkennung ist ein anderer Aspekt. Signaturen können nicht alles abdecken. Das bedeutet aber nicht, dass sie ineffektiv sind, denn sie liefern wertvolle Informationen.

„Antivirus" im Sinne eines „Antivirenprogramms" ist wiederum ein anderer Aspekt. Ja, solche Programme sind meist signaturbasiert, aber seit Anfang der 90er Jahre haben sich fast alle Lösungen weiterentwickelt und beinhalten zusätzliche Technologien wie Heuristik, Cloud-basierte Ansätze und viele weitere Sicherheitsfunktionen.

WIE IST ES UM MEINE ERWEITERTEN MALWARE-ERKENNUNGSFÄHIGKEITEN BESTELLT?

Mit dem folgenden Experiment können die erweiterten Erkennungsmöglichkeiten einfach getestet werden:

1. Installieren Sie ein Antivirenprogramm
2. Aktualisieren Sie die Signaturen nicht
3. Scannen Sie aktuelle Malware und sehen Sie, was passiert.

Es ist überraschend, was zum Beispiel rein heuristische Technologien alles erkennen können. In vielen Fällen wird bis zu 80 % der aktuellen Malware erkannt. Signaturen machen daher in diesen Produkten die Arbeit nicht alleine, aber bieten eine hervorragende Unterstützung.

Auf die gleiche Weise wie die „bösen Jungs" erwachsen geworden sind, haben sich auch die „guten Jungs" weiterentwickelt, um den sich laufend ändernden Anforderungen der Cybersicherheit gerecht zu werden. Dazu sind viele verschiedene Technologieansätze erforderlich, um alle Bedrohungen zu erkennen.

Von „veralteten" Signaturen bis hin zu modernem maschinellem Lernen: Der ständige Wandel der Cyber-Bedrohungen ist ein guter Grund dafür, verschiedene Ansätze zu kombinieren, anstatt sich auf einen einzigen Ansatz zu verlassen.

6 FAZIT

In einer Zeit, in der das tägliche Datenvolumen schnell und in beispiellosem Ausmaß wächst, sind immer ausgefeiltere Lösungen erforderlich, um die Daten von Unternehmen und Einzelpersonen vor Angriffen zu schützen. Die Anzahl der Bedrohungen steigt stark an eine Kurve, die mit jedem Jahr noch steiler wird. Ebenso entwickeln sich die Angriffsformen ständig weiter. Nur begrenzt durch den Einfallsreichtum der Angreifer und die Leistungsfähigkeit der ihnen zur Verfügung stehenden Technologien Technologien, die sich ähnlich schnell weiterentwickeln.

Die finanziellen und rechtlichen Risiken für Unternehmen, die sich durch mangelnde IT-Sicherheit ergeben, sind zu hoch, um sie zu ignorieren. Präventivmaßnahmen, Mitarbeiterschulungen und klassische Strategien zur Erkennung von Bedrohungen durch einzelne Hersteller tragen alle zum Schutz bei. Dies allein reicht jedoch nicht aus, um die immer komplexeren Bedrohungen zu bekämpfen, mit denen Unternehmen inzwischen täglich konfrontiert sind.

Tabidus hat sich mit Mut und Erfindungsreichtum der Entwicklung von Sicherheitsstrategien verschrieben, die die Ansätze der Cyberkriminellen übertreffen. Wir können uns dabei nicht allein auf die Strategien verlassen, die in der Vergangenheit ihren Zweck erfüllt haben. Denn sie sind schlicht und ergreifend nicht mehr ausreichend für unser digitales Zeitalter. Eine agile Herangehensweise an die Cybersicherheit, die ein Teamwork zwischen den Anbietern erlaubt und dabei die maximale Leistung aus den gebündelten Kräften schöpft, ist unserer Meinung nach der Ansatz, der den besten Schutz für Unternehmen verspricht heute und in der Zukunft.

VIELEN DANK

NEHMEN SIE KONTAKT AUF:

+43 1 348 5005

office@tabidus.com

www.tabidus.com

@TabidusTech

TABIDUS
TECHNOLOGY
UNITED MALWARE PROTECTION