Zentral verwaltete Sicherheits-infrastruktur in der Cloud

Dr. Götz Güttich

Mit "Trend Vision One" bietet Trend Micro eine einheitliche, zentral verwaltete Sicherheitslösung für Unternehmensumgebungen an. Mit dem Produkt möchte der Hersteller Silos aufbrechen und ein einziges Werkzeug bereitstellen, mit dem sich Risiken identifizieren und bewerten lassen. Damit nicht genug, kann die Lösung auch die Assets im Netz inventarisieren und Bedrohungen gleichermaßen in E-Mails, Endpoints, Servern, Cloud-Infrastrukturen und Netzwerken erkennen und bekämpfen. Wir haben Trend Vision One im Testlabor unter die Lupe genommen.

Trend Vision One lässt sich sowohl zum Attack Surface Management (ASM), als auch für Extended Detection and Response (XDR) nutzen. Die Konfiguration und die Überwachung der Lösung finden über eine Cloud-basierte Konsole statt. Im Betrieb verteilen die Administratoren die Agenten zum Schutz der einzelnen Komponenten auf die Rechner im Netz. Das können sowohl interne Assets, als auch Geräte, die aus dem Internet erreichbar sind, sein. Die Security-Produkte laufen dann auf den einzelnen Systemen und sorgen nicht nur mit Funktionen wie Antivirus und Firewall für deren Sicherheit, sondern sammeln auch Informationen und Telemetriedaten, die sie dann wiederum dem zentralen Managementwerkzeug zur Verfügung stellen. Dort werden sie mit Daten aus globalen Threat-Intelligence-Feeds und Drittanbieterinformationen kombiniert, um ein möglichst vollständiges Bild zu erhalten.

Die IT-Verantwortlichen haben anschließend die Option, die Daten auszuwerten und einen Risikoindex mit XDR-Erkennungen, kompromittierten Konten, Vulnerabilities, Fehlkonfigurationen und Ähnlichem zu erstellen. Dieser lässt sich bei Bedarf an verschiedene Zielgruppen wie CEOs und CSOs anpassen und es besteht sogar die Möglichkeit, Vergleiche zu anderen Organisationen zu ziehen.

Abgesehen davon lassen sich die Risiken auch automatisch priorisieren und automatische Reaktionen auf erkannte Bedrohungen und Risiken definieren. Um eine breite Perspektive und einen erweiterten Kontext zur Verfügung zu stellen, kommen sowohl Machine-Learning-Funktionen, als auch fortgeschrittene Sicherheitsanalysen zum Einsatz.

Da alle Daten im Unternehmen von der gleichen Plattform gesammelt und verarbeitet werden, kommt es zu keinen ineffektiven Datenübertragungen zwischen Drittanbieterlösungen und alle Informationen sind stets vollständig und konsistent. IT-Verantwortliche erhalten demzufolge sämtliche Informationen und Werkzeuge, die sie benötigen, um ihre Umgebungen bestmöglich abzusichern und die Zahl der False Positives zu minimieren.

Im Betrieb übernimmt Trend Vision One folglich nicht nur die

pausenlose Bedrohungserkennung, sondern liefert auch ständig intelligente Empfehlungen darüber, wie die Administratoren mit den gefundenen Bedrohungen umgehen sollten. Bei sämtlichen zur Verfügung stehenden Informationen besteht zudem die Möglichkeit, in die Tiefe zu gehen und beispielsweise Vulnerabilities oder auch einzelne Assets im Detail zu analysieren, auch über den Zeitverlauf hinweg. Auf diese Art und Weise lässt sich der gesamte Ablauf eines Angriffs visualisieren.

Die Inbetriebnahme der Lösung

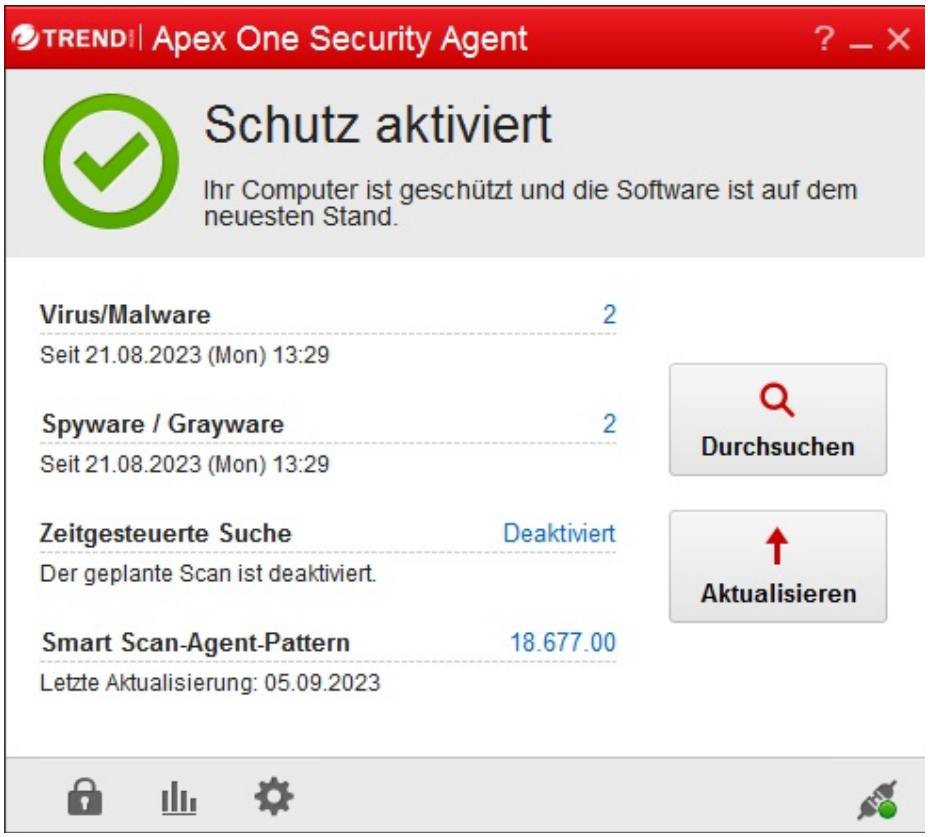
Da Trend Micro seinen Kunden für die Inbetriebnahme der Lösung einen IT-Spezialisten aus eigenem Hause oder von einem Partnerunternehmen zur Verfügung stellt, läuft der genannte Vorgang ziemlich reibungslos ab. Im Test wurden wir zunächst aufgefordert, unter https:// resources. trendmicro. com/ vision-one-trial-de.html einen Test-Account anzulegen. Danach war es erforderlich, die Region für das zu verwendende Rechenzentrum festzulegen, im Test wählten wir zu diesem Zeitpunkt "Deutschland" aus. Anschließend wurde die Konsole erstellt, ein Vorgang, der nach ein paar Minuten abgeschlossen war.

Nach dem ersten Login bei der Management-Konsole startete zunächst einmal ein Assistent, der die Anwender auf die wichtigsten Punkte hinweist. Da wir Support direkt von Trend Micro hatten, ließen wir diesen Assistenten zu diesem Zeitpunkt links liegen und gingen stattdessen direkt daran, die benötigten Produktinstanzen zu erstellen. Dazu wechselten wir nach "Service Management / Product Instance" und erzeugten Instanzen zum Endpoint-Schutz für Clients sowie für Server und Workloads.

Im nächsten Schritt ging es an die Erstellung und Installation der Agentensoftware für die Endpoints. Dazu gingen wir nach "Endpoint Security Operations / Endpoint Inventory" und erstellten dort zwei Pakete, eines für Windows Clients und eines für Windows Server. An sonstigen Betriebssystemen unterstützt Trend Vision One auch macOS bei den Standard-Endpoints und Linux bei den Servern. Bei Bedarf ist es auch möglich, nur Sensoren im Netz zu verteilen, die keine Schutzfunktionen mitbringen und nur Daten sammeln, beispielsweise zum Überwachen von Office 365, von mobilen Geräten und Ähnlichem.

Die Verteilung der Software erfolgt dann im Betrieb entweder manuell, oder über eine Deployment-Lösung. Wir spielten den Agenten auf unseren Clients unter Windows 10 und 11 sowie auf unseren Servern unter Windows Server 2019 ein. Das System lässt sich dabei auch so konfigurieren, dass die Agenten bei der Installation auch gleich die Policy mit laden.

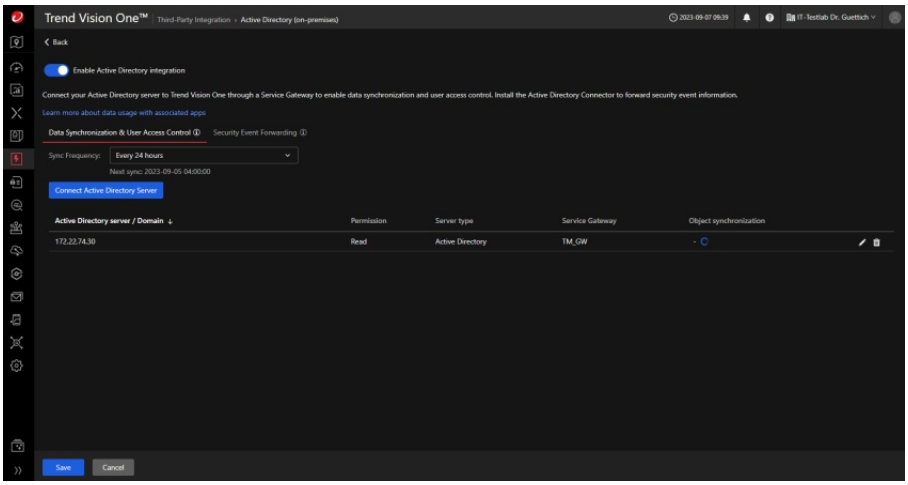
Für unsere Policy verwendeten wir im Test die Trend-Micro-Vorlage "Best Practice". Diese stellt nach Angaben des Herstellers zwar nicht den höchsten Sicherheitsstandard dar, liefert aber eine gute Grundsicherheit und erzeugt im Netz keine Probleme. Es ergibt deswegen Sinn, sie nach Neuinstallationen zunächst einmal in Betrieb zu nehmen und sie dann nach Bedarf nachzuschärfen. Im Test gingen wir genauso vor und aktivierten zusätzlich noch die Intrusion Prevention, das Integrity Monitoring und die Log Inspection.



Die Agenten-Software auf dem Client

Als das erledigt war, wechselten wir nach “Administration” und erzeugten einen Scheduled-Task, der die Software alle zwölf Stunden über den Trend-Micro-ActiveUpdate-Server aktualisierte. Zum Schluss wiesen wir unsere Policies noch den Endpoints zu. Daraufhin nahm die Agentensoftware ihre Arbeit auf.

Im Betrieb fand sie zunächst einmal diverse infizierte Dateien und Fehlkonfigurationen in Bezug auf Konten und Geräte bei uns im Netz. Wir lösten diese Probleme dadurch, dass wir die betroffenen Dateien entfernten



Unser lokales Active Directory bei der Synchronisation über den Service Gateway

und die Konfigurationen entsprechend der Trend-Micro-Empfehlungen und unserer Anforderungen anpassten.

Das Einbinden des Active Directory

Nachdem die gefundenen Probleme gelöst waren, gingen wir zum nächsten Schritt über. In unserem Testlabor verwendeten wir ein On- Premises- Active- Directory, das wir mit seinen Daten gerne in die Trend-Vision-One-Umgebung integrieren wollten. Dazu mussten wir einen so genannten Service Gateway bei uns im Netz einrichten, der unter anderem die Aufgabe übernahm, die Verbindung zwischen dem lokalen Active Directory und der Cloud herzustellen. Dazu steht unter “Workflow and Automation” der Punkt “Service Gateway Management” zur Verfügung. Dort lässt sich eine Virtuelle Maschine (VM) für die Hypervisoren “Vmware ESXi” oder “Microsoft Hyper-V” herunterladen. Im Test verwendeten wir die Vmware-Version, die wir auf einem ESXi-8.0-Update-1-System ans Laufen brachten. Der Hersteller empfiehlt für die bei uns verwendete Konfiguration übrigens den Einsatz von vier virtuellen CPUs und acht Gbyte Speicher.

Nachdem die VM, die auf Centos 7 basiert, hochgefahren war, konnten wir uns mit den Standard-Credentials “admin/V1S-G@2021” bei dem System anmelden. Danach mussten wir zunächst einmal ein neues Passwort vergeben und fanden uns anschließend auf einer Kommandozeile wieder. Um in den Konfigurationsmodus zu gelangen, mussten wir den Befehl “enable” eingeben. Danach konnten wir – ebenfalls über die Kommandozeile – die Netzwerkkonfiguration vornehmen, den Hostnamen setzen und mit dem Befehl “connect” die Internetanbindung überprüfen. Danach war es noch erforderlich, die VM mit Hilfe eines Tokens, das uns über das Web-basierte Managementwerkzeug zur Verfügung gestellt worden war, zu registrieren. Nach dem Abschluss dieses Vorgangs, der in der Beschreibung komplizierter klingt, als er in Wirklichkeit war, ist der Service Gateway einsatzbereit und kann konfiguriert werden.

Im Test wechselten wir jetzt nach “Workflow and Automation / Third Party Integration / Active Directory (on-premises)” und aktivierten die entsprechende Funktion. Anschließend legten wir die Synchronisierungsfrequenz fest und verbanden das System mit unseren Active-Directory-Servern. Nach einem Verbindungstest und einem Klick auf “Connect” und “Save” konnten Trend Vision One und unser lokales Active Directory miteinander kommunizieren und beispielsweise Benutzerdaten austauschen.

Weitere Daten in Trend Vision One einbinden

Neben der Datenübermittlung aus dem Active Directory durch die eben geschilderte Integration – beispielsweise für das Risk Assessment – lassen sich auch noch die Windows Event Logs der Active-Directory-Controller an Trend Vision One übermitteln. Die Daten erscheinen dann im System als Detection Logs und reichern die XDR Workbenches und Observed Attack Techniques an.

Um diese Log-Übermittlung zu aktivieren, wechselten wir im Test zunächst nach “Workflow and Automation / Service Gateway Management” und klickten dort auf “Manage API Key”.

Dann kopierten wir den bereits erzeugten Key in eine Textdatei und verschoben diese auf unseren Active-Directory-Server. Anschließend gingen wir nach "Workflow and Automation / Third Party Integration / Active Directory (on-premises)" und selektierten den Reiter "Security Event Forwarding". Dort konnten wir den Installer für den entsprechenden Agenten (zum Testzeitpunkt war Version 1.0.0.10032 aktuell) herunterladen und auf dem Active-Directory-Server ausführen.

Nach dem Abschluss der Installation mussten wir den Agenten nur noch konfigurieren. Dazu teilten wir ihm die Adresse des Service Gateway mit und kopierten den API Key in das dazugehörige Dialogfeld. Nach einem kurzen Verbindungstest, der positiv verlief, klickten wir auf "Connect" und die Verbindung kam zustande. Zum Abschluss mussten wir nur noch im Web-Interface auf dem Reiter "Security Event Forwarding" die automatischen Updates aktivieren, danach war das System betriebsbereit.

Über die „Third-Party-Integration" lassen sich viele zusätzliche Informationsquellen einbinden

Simulierte und andere Angriffe

Ungewöhnlich ist, dass Trend Micro den Anwendern Demo-Skripts zur Verfügung stellt, mit denen sie testen können, wie Trend Vision One auf erkannte Angriffe reagiert. Die Simulationen beziehen sich auf die Bereiche "Workbench" und "Observed Attack Techniques". Hier finden sich jeweils die Einträge "Endpoint Attack Szenario", "Network Attack Szenario" und "Email Attack Szenario". Im Test ließen wir zu diesem Zeitpunkt den Endpoint-Angriff laufen. Dieser simuliert den Vorgang, den SAM-Hive aus der Windows Registry auszulesen und die NTDS-Datei zu kopieren. Kurz nachdem wir das Demo-Skript mit dem Angriff – das wir zuvor von Trend Micro heruntergeladen hatten – auf dem Client ausgeführt hatten, erschienen die erkannten Angriffe wie erwartet in der Workbench-App im Web-Interface. Das System funktionierte also einwandfrei. Auf die Workbench-App gehen wir im späteren Testverlauf noch genauer ein.

Im Test beschränkten wir uns zu diesem Zeitpunkt allerdings nicht auf die Demo-Skripts des Herstellers, sondern verwendeten diverse Sicherheitswerkzeuge, wie beispielsweise Metasploit, um Daten aus den von Trend Micro geschützten Testsystemen auszulesen. Auch hier wurden wir nach kürzester Zeit im Web-Interface der Lösung wegen der laufenden Angriffe gewarnt.

Der Leistungsumfang des Verwaltungswerkzeugs

Gehen wir jetzt einmal genauer auf den Leistungsumfang des Management-Tools ein, um einen Überblick über den Funktionsumfang von Trend Vision One zu erhalten. Nach dem Login landet der Administrator in einem Dashboard, das ihm einen Überblick über den aktuellen Risk Index seiner Umgebung bietet. Dieser setzt sich aus verschiedenen Risikofaktoren zusammen, zu denen unter anderem die Sicherheitskonfiguration des Netzwerks und das Angriffsrisiko gehören. Ausgehend von dieser Information sind die zuständigen Mitarbeiter dann dazu in der Lage, Maßnahmen zu treffen, die das Sicherheitsniveau verbessern.

An gleicher Stelle finden sich noch diverse andere Übersichten. Der "Exposure Index" zeigt Verwundbarkeiten und Fehlkonfigurationen und setzt sie in Relation zu den Verhältnissen in anderen Organisationen. Hier finden die Administratoren beispielsweise heraus, wie lang es im Durchschnitt dauert, bis Patches im Unternehmen und im globalen Durchschnitt eingespielt wurden und wieviel Prozent der Endpoints CVEs enthalten, die ausgenutzt werden könnten, auch hier wieder in Bezug auf das Unternehmen und die weltweite Situation.

Die "Attack Overview" informiert im Gegensatz dazu über die erfolgten Angriffe. Dazu gehören

beispielsweise gefundene Viren, Privilegeskalationen oder auch laterale Bewegungen. Die "Sicherheitskonfiguration" gibt wiederum Aufschluss über den Status der Endpoint Protection im Unternehmen. Hier sehen die zuständigen Mitarbeiter, ob die Agenten-Software auf ihren Geräten aktuell ist und welche Funktionen – wie beispielsweise Behaviour Monitoring oder Firewall – aktiviert wurden.

Die "Attack Surface Discovery" zeigt die im Unternehmen vorhandenen Geräte und ermöglicht es auch, auf Geräteeinträge in der Liste zu wechseln und Detailinformationen zu den einzelnen Devices abzurufen. Dazu gehören unter anderem das "Risc Assessment" und die auf dem Gerät sichtbaren Nutzerkonten. Abgesehen davon liefert die Attack Surface Discovery unter anderem auch Informationen über Assets und die auf dem jeweiligen System genutzten Cloud-Applikationen.

Das "Operations Dashboard" gibt Tipps zum Verringern des Risikoindex. Dazu werden die Risikofaktoren kategorisiert, um einen besseren Einblick in die verwundbaren Geräte, Anwendungen und Cloud Apps zu geben. Die Tipps zeigen dann in der Praxis beispielsweise, wie die Agentensoftware auf den Endpoints im Idealfall konfiguriert sein sollte. Die Liste der Risikofaktoren umfasst alle gefundenen Probleme, wie Fehlkonfigurationen bei Administratorkonten, fehlerhafte Systemkonfigurationen, erkannte Angriffe und Ähnliches in Listenform mit Tipps, wie sie sich beheben lassen. Das ist sehr nützlich, um die Umgebung schnell abzusichern.

Die anderen Bereiche der Verwaltungsoberfläche sind über Menüpunkte auf der linken Fensterseite erreichbar. Zunächst einmal gibt es hier ein Inhaltsverzeichnis der gesamten Plattform, über das sich alle Funktionen direkt aufrufen lassen und in dem sie nach Aufgabenbereich kategorisiert wurden.

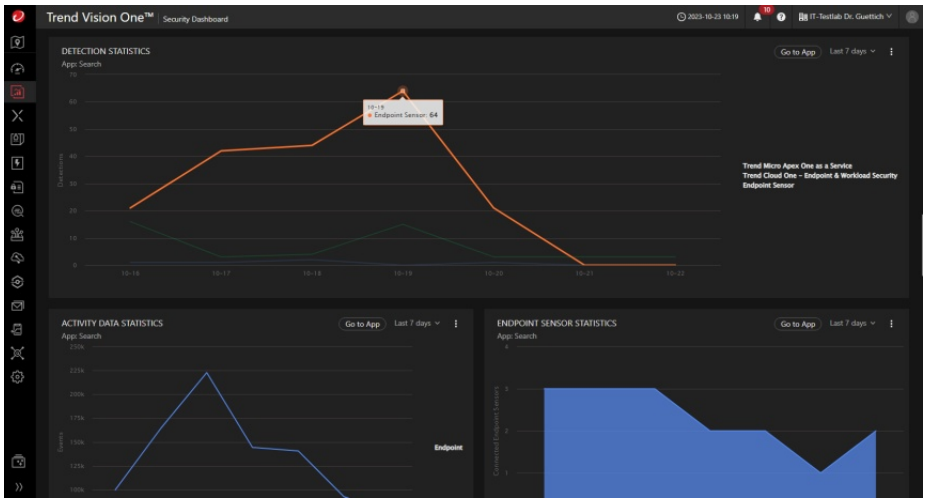
Die Dashboards und Reports

Etwas interessanter ist der Menüpunkt "Dashboards and Reports". Das darin enthaltene "Security Dashboard" lässt sich mit Widgets genau an die Anforderungen der jeweiligen Umgebung anpassen. Insgesamt stehen hier 30 Widgets bereit, die über die Aktivitätsdaten, die Statistiken der Endpunktsensoren, die Erkennungen nach Angriffstypen, die IP-Adressen mit der größten Filteraktivität und vieles mehr informieren.

Was die Reports angeht, so stehen 25 unterschiedliche Templates zur Verfügung, die Informationen liefern zu Risiken, Konten, Aktivitätslogs, verfügbaren Endpoints, internen Anwendungen, mobilen Geräten und Ähnlichem. Bei Bedarf besteht aber immer die Option, eigene Reports anzulegen. Die IT-Mitarbeiter können Reports auch automatisch zu bestimmten Zeiten erzeugen, mit einem Logo an die Corporate Identity anpassen und sie automatisch an bestimmte Adressen mailen.

Die XDR Threat Investigation und die Workbench-App

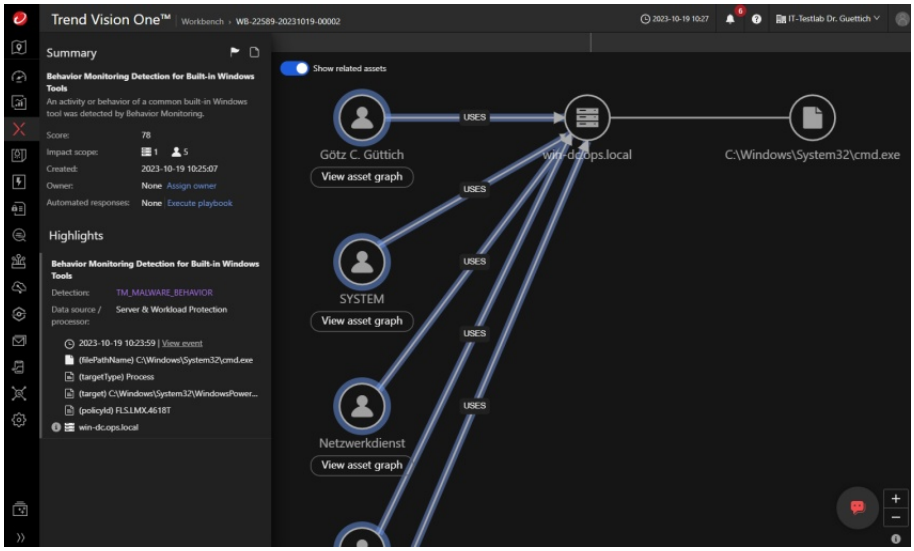
Die "XDR Threat Investigation" ermöglicht es den Administratoren, bestimmte Erkennungsmodelle – wie zum Beispiel die Erkennung verdächtiger Tools oder das Erkennen von mit Fremdcode überschriebenen, ausführbaren Windows-Dienstdateien – zu aktivieren oder zu deaktivieren. An gleicher Stelle lassen sich auch Ausnahmen definieren.



Das konfigurierbare „Security Dashboard" bietet einen schnellen Überblick über die wichtigsten Punkte

Unter dem gleichen Menüpunkt steht auch die so genannte Workbench App zur Verfügung. Sie ist ein zentraler Bestandteil von Trend Vision One. Hier finden sich die Alarme sowie die Vorfälle und die Administratoren haben Gelegenheit, festzustellen, was sie ausgelöst hat und was für Ereignisse und Indikatoren mit ihnen zusammenhängen. Eine grafische Darstellung visualisiert dabei die Beziehungen zwischen

den einzelnen, mit dem Alarm zusammenhängenden Objekten. Bei Bedarf lassen sich die Objekte in dieser Grafik auch per Drag-and-Drop anordnen, um die Übersichtlichkeit zu erhöhen. Weitere Informationen sind über einen Rechtsklick abrufbar und die Administratoren können auch direkte Aktionen starten, wie die Isolierung von Endpoints oder auch das Deaktivieren von Benutzerkonten. Analog zur Workbench gibt es auch eine App, die Angriffstechniken anzeigt, die im Netz erkannt wurden. Hier lässt sich die Anzeige auch filtern, beispielsweise nach Zeitraum oder Risiko-Level.



Die Angriffe werden auch grafisch visualisiert

"Threat Intelligence" informiert die zuständigen Mitarbeiter über aktuelle Bedrohungen. Die diesen Informationen zugrundeliegenden Daten kommen – wie gesagt - aus internen und externen Quellen, also nicht notwendigerweise nur von Trend Micro.

Playbooks ermöglichen automatische Reaktionen

Im Bereich "Workflow and Automation" findet sich der Punkt "Security Playbooks". Für die Playbooks, die dazu dienen, um automatisch – beispielsweise durch Endpunktisolationen – auf plötzlich auftretende Risiken oder Sicherheitsvorfälle zu reagieren, stehen diverse Templates bereit. Beispielsweise zum Herausfinden der Risiken beim Konfigurieren der Konten oder auch zum Starten eines Skripts. Wir untersuchten im Test zu diesem Zeitpunkt unsere internen Assets auf CVEs mit globaler Exploit-Aktivität. Dazu selektierten wir das dazugehörige Template. Daraufhin zeigte uns das System den Aufbau des Templates in grafischer Form mit Auslöser, Zielsystemen und den Bedingungen anhand derer dann diverse Aktionen durchgeführt werden und ermöglichte es uns, das Template zu bearbeiten. Im nächsten Schritt konnten wir aus dem Template ein Playbook erzeugen und dieses aktivieren. Im Test ergaben sich dabei keine Probleme.

Ebenfalls von Interesse: das Response Management. Hier lassen sich Powershell- und Bash-Skripts hinterlegen, die unterschiedliche Aufgaben ausführen können, beispielsweise das Stoppen von Prozessen. Die "Third Party"-Integration ermöglicht es im Gegensatz dazu, externe Anwendungen in die Sicherheitsumgebung einzubinden und so zusätzliche Daten zu importieren, die die Visibilität der Gesamtumgebung verbessern. Das System kommuniziert dabei nicht nur mit dem von uns bereits erwähnten Active Directory, sondern auch mit vielen anderen Quellen, wie beispielsweise Office 365, LogRhythm SIEM, Qualys oder auch Syslog-Servern. Punkte zum Verwalten des RESTful API und dem bereits erwähnten Service Gateway Management schließen den Bereich "Workflow and Automation" ab.

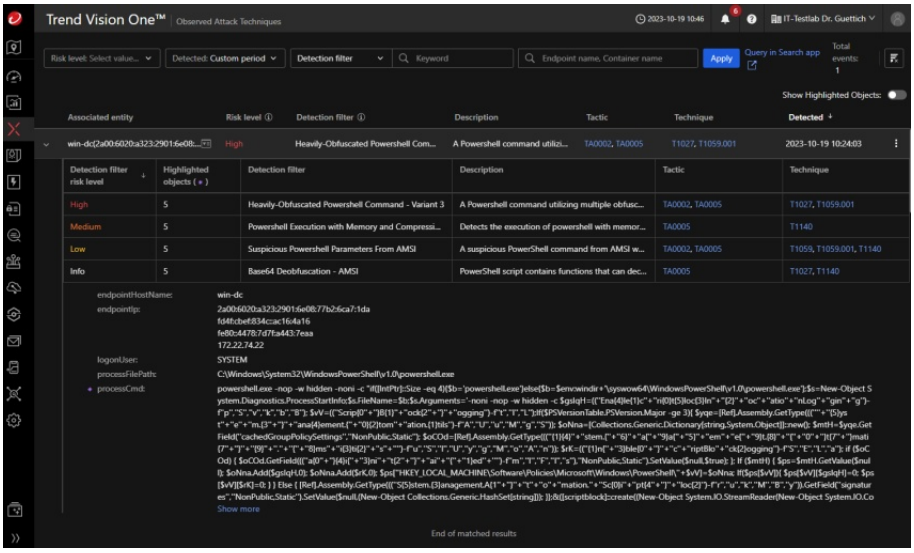
Zero Trust und Cyber Risk Assessment

Über den Zero-Trust-Secure-Access aktivieren die IT-Verantwortlichen diverse Sicherheitsfunktionen, die beispielsweise den Internet-Zugriff und die Arbeit mit internen Anwendungen steuern und überwachen. Das "Cyber Risk Assessment" dient dazu, die Anfälligkeit der Unternehmensumgebung in Bezug auf kürzlich aufgetretene Globale Bedrohungen unter die Lupe zu nehmen. Damit lassen sich beispielsweise Phishing-Angriffe simulieren, Endpoints auf Risiken hin scannen oder auch Mails überprüfen. Im Test ergaben sich dabei keine Schwierigkeiten. Wir konnten beispielsweise mit Hilfe des dazugehörigen Assistenten eine Demo-Phishing-Mail und ein entsprechendes Portal erstellen, die Empfänger der Phishing-Mails auswählen und die Kampagne starten. Anschließend lief sie in unserem Test problemlos ab.

Die "Endpoint Security Operations" stellen ein weiteres Herzstück des Systems dar, denn sie bieten die genannten Funktionen

zum Absichern der Endpoints. Hier finden sich die Systeme, auf denen der Trend-Micro-Agent läuft und es besteht die Möglichkeit, die Policies für Server und Workstations zu definieren und zuzuweisen.

An gleicher Stelle sind auch Dashboards verfügbar, die über aktuelle Bedrohungen auf den jeweiligen Systemen informieren, außerdem lassen sich hier auch Logs und Reports einsehen. Ein Administrationsbereich mit Alarm-, Agenten- sowie Updateverwaltung und Ähnlichem



Details zu einem Angriff mit verschleierten Powershell-Befehlen

schließt den Leistungsumfang der Endpoint-Sicherheit ab.

E-Mail- und Mobile-Security

Über die E-Mail-Sicherheitsfunktion werden Administratoren in die Lage versetzt, E-Mail-Aktivitäten unter Gmail und Microsoft 365 zu überwachen. Die Mobile Security Operations ermöglichen es im Gegensatz dazu unter anderem, ein Inventory der mobilen Geräte zu erstellen, mobile Policies zu definieren und Mobile Detection Logs einzusehen. Trend Vision One erkennt also gefährliche Anwendungen und Dateien auf den mobilen Devices, identifiziert unsichere Geräte und Betriebssysteme und schützt die Anwender vor Bedrohungen aus dem Web und vor Phishing. Unterstützt werden dabei die Betriebssysteme Android, ChromeOS und iOS.

Unter "Service Management" lassen sich die Produktinstanzen wie "Standard Endpoint for Clients" oder "Server and Workload" verwalten und "Administration" ermöglicht die Verwaltung von Trend Vision One an sich. Hier legen die Administratoren Benutzerrollen fest, erzeugen Benutzerkonten, verwalten API Keys, konfigurieren Alarmmeldungen und sehen Audit Logs ein. Darüber hinaus legen sie die Zeitzone fest, limitieren die Zugriffe auf die Konsole auf bestimmte IP-Adressen, sammeln Daten für den Support, untersuchen, wie viele Credits ihnen noch für die Aktivierung von Funktionen zur Verfügung stehen und Ähnliches.

Hilfe durch die KI

Der „Companion" von Trend Micro stellt eine integrierte KI-Lösung dar, die bei der Suche hilft, Alarme erklärt, Aktionen empfiehlt und komplexe Skripts dekodiert. Da die Lösung derzeit noch als Preview gekennzeichnet ist, haben wir sie nur angetestet und nicht tiefgehend analysiert. Wir verwendeten sie beispielsweise, um uns Befehle erklären zu lassen, die zu Alarmen geführt haben. Der Companion macht schon jetzt einen durchaus positiven Eindruck und wird sicher in Zukunft Administratoren viel Zeit sparen können.

Fazit

Mit Trend Vision One bietet Trend Micro eine ganzheitliche Sicherheitslösung für Unternehmen an, die vor allem durch ihren großen Funktionsumfang überzeugt. Sie ermöglicht es nicht nur, Server, Endpoints und Mobilgeräte zu schützen, sondern sammelt bei Bedarf auch im ganzen Unternehmensnetz und der in Cloud Informationen zu sicherheitsrelevanten Vorfällen. Die IT-Verantwortlichen können sowohl Alerts generieren lassen, oder sich direkt über das Web-Interface über den aktuellen beziehungsweise den vergangenen Status informieren.

Nützlich sind die Playbooks, die automatische Reaktionen auf Sicherheitsvorfälle ermöglichen. Das gleiche gilt für die Einbindung externer Informationen, mit denen sich die Administratoren über laufende Sicherheitsbedrohungen informieren können, bevor sie ihr Unternehmen erreichen. Mit den ganzen Funktionen und der Option, über das Web-Interface aktiv Gegenmaßnahmen gegen Angriffe zu ergreifen, kann Trend Vision One enorm beim Erhöhen des Sicherheitsniveaus helfen. IT-Spezialisten, die nach einer ganzheitlichen Security-Lösung suchen, sollten das Produkt auf jeden Fall in die engere Wahl einbeziehen.