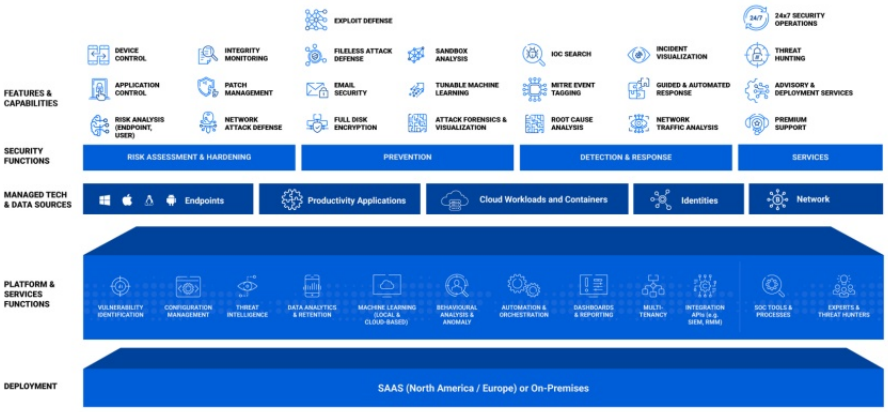
Ganzeheitliche Sicherheitslösung für Unternehmensumgebungen

Dr. Götz Güttich

Mit GravityZone Business Security Enterprise bietet Bitdefender eine Sicherheitslösung an, die Security-Probleme erkennt und darauf reagieren kann. Das Produkt fällt vor allem durch seine ausgefeilten Visulisierungsfunktionen auf und steht für Unternehmen aller Größen zur Verfügung. Wir haben uns im Testlabor angesehen, wie die Inbetriebnahme abläuft, welchen Leistungsumfang es mitbringt und wie es sich bei der täglichen Arbeit verhält.

GravityZone Business Security Enterprise wird über ein zentrales Web-Interface verwaltet und überwacht. Auf diese Art und Weise steht den Administratoren ein einheitliches Security-Portal zur Verfügung, über das sie nicht nur den Status ihrer Komponenten einsehen können, sondern auch dazu in der Lage sind, administrative Aufgaben durchzuführen. Um einen detaillierten Überblick zu erhalten, können die IT-Verantwortlichen zudem ein frei konfigurierbares Dashboard verwenden. Im Test verwendeten wir die Cloud-Variante von GravityZone, es existiert aber auch eine Version für den Einsatz on-premises.

Das System setzt auf den zu schützenden Endpoints lokale Security-Komponenten ein, die „Bitdefender Endpoint Security Tools“. Diese überwachen nicht nur die jeweils betroffenen Systeme, sondern sind auch in Kombination mit zusätzlichen Sensoren dazu in der Lage, über das Netz zusammenzuarbeiten und so Bedrohungen sichtbar zu machen, die sich über mehrere Endpoints erstrecken.



Auf diese Weise liefern sie erweiterte Einsichten in den Sicherheitsstatus der gesamten IT-Umgebung, erkennen Bedrohungen automatisch und reagieren in vielen Fällen auch gleich darauf. So erhöhen sie das Sicherheitsniveau der IT-Umgebungen deutlich. GravityZone Business Security Enterprise schützt sowohl physisch vorhandene Netzwerkgeräte, als auch virtuelle Umgebungen und Cloud-Plattformen. Die Endpoint Security Tools stehen für die Betriebssysteme Linux, MacOS und Windows zur Verfügung.

Besserer Durchblick für Administratoren

Umfassende Analyse-Tools helfen den IT-Verantwortlichen im Betrieb dabei, den Überblick zu behalten. Da die Lösung sonst getrennte Warnmeldungen zusammenführen kann, erweitert sie den Überblick über die Infrastruktur um viele wichtige Informationen. Zu den dabei überwachten Komponenten gehören neben den bereits genannten auch die Bereiche E-Mail und Identität. GravityZone stellt damit eine vollständige Sicherheitslösung aus einer Hand dar, die die Security-Bedürfnisse des ganzen Netzes abdeckt und eine Echtzeitüberwachung ermöglicht.

Findet ein Angriff statt, so legt GravityZone das Angriffsgeschehen offen. Es gibt sowohl eine grafische Darstellung der einzelnen Aktionen in Form eines Diagramms, als auch eine tabellarische Übersicht über die Ereignis-

se. Dazu kommen dann noch andere Daten wie Ursachenanalysen, Reaktionsempfehlungen und Kontextinformationen.

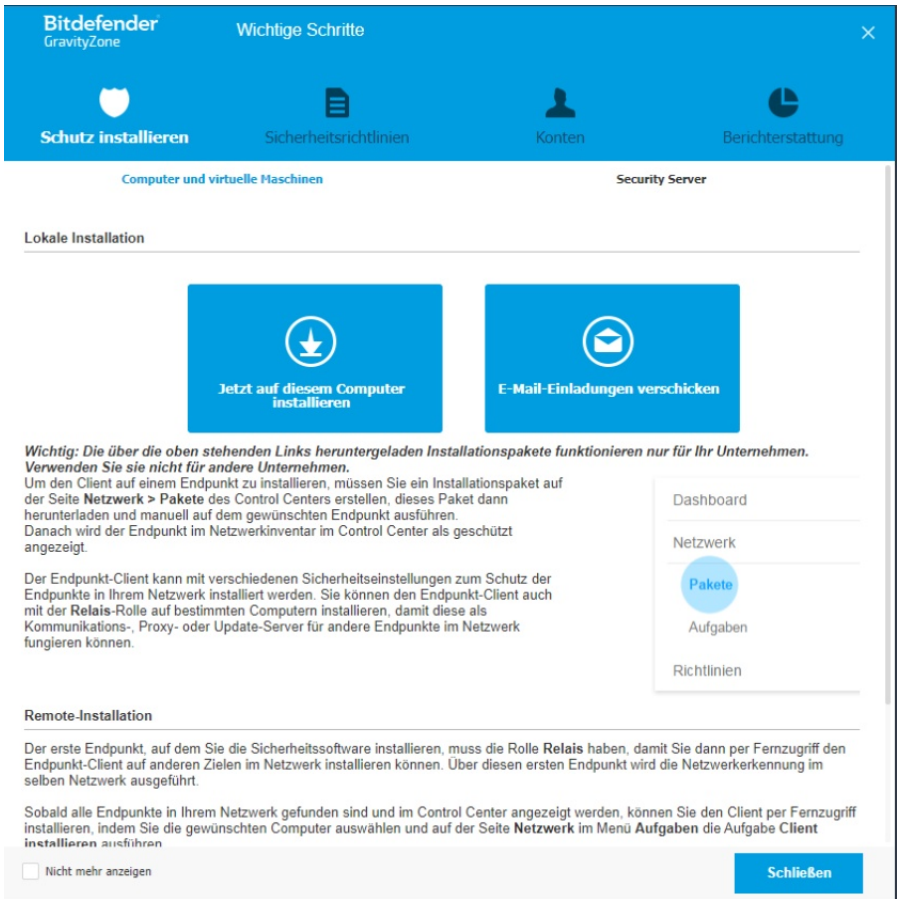
Die verwendeten Erkennungsalgorithmen werden sowohl lokal als auch in der Analyseplattform von GravityZone bereitgestellt. Bei Bedarf gibt es auch die Option, eigene Erkennungsregeln hinzuzufügen.

Was die Zusatzsensoren angeht, die getrennt lizenziert werden müssen, so bietet GravityZone Sensoren für Office 365, AWS, Active Directory, Azure-AD, Microsoft Intune, Azure und Google Workspace an. Dazu kommt noch ein Netzwerksensor, der die Datenübertragungen im Netz im Auge behalten kann. Dieser wurde in Form einer virtuellen Maschine realisiert und benötigt einen Einblick in den Netzwerk-Traffic über einen Mirror-Port.

Der Test

Im Test stellte uns Bitdefender einen Account für GravityZone zur Verfügung und schaltete diverse Lizenzen frei, so dass wir Business Security Enterprise in der vollen Ausbaustufe mit XDR (Extended Detection and Response) einsetzen konnten. Wir richteten das System anschließend in unserem Netzwerk ein und führten zunächst einmal einen Sicherheits-Scan durch. Dabei wurden einige Probleme gefunden und gelöst. Die Agenten auf den Endpoints fanden diverse Testdateien, die wir für Security-Tests verwendeten sowie unterschiedliche Werkzeuge von Nirsoft und Sysinternals, die ihnen suspekt vorkamen und verschoben diese in Quarantäne beziehungsweise löschten sie komplett. Das lief bei uns alles ohne Interaktion mit dem Administrator ab.

Danach aktivierten wir die Sensoren zur Überwachung des AD und den Netzwerksensor, um einen möglichst vollständigen Überblick über die Aktivitäten in unserem Netz zu erhalten. Anschließend ließen wir das System laufen, machten uns mit seinem Leistungsumfang bekannt und analysierten, wie die tägliche Arbeit mit der Lösung ablief.



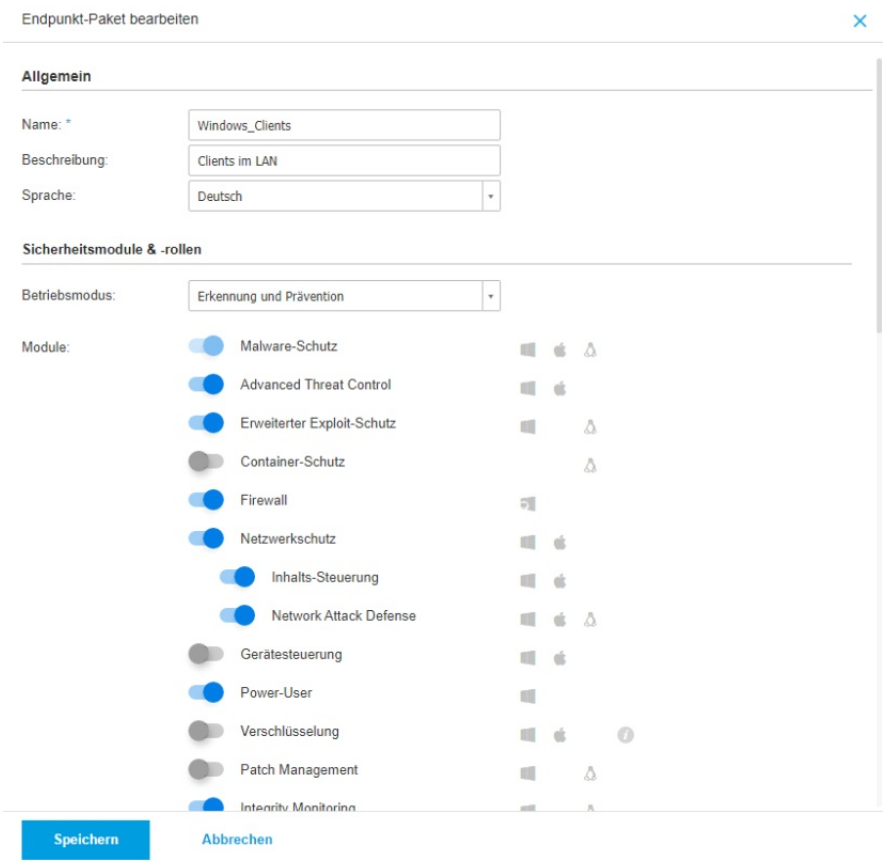
Nach dem Login beim Webinterface hilft eine Informationsseite beim Einrichten von GravityZone

Inbetriebnahme der Agenten auf den Endpoints

Zu Beginn des Tests loggten wir uns mit unserem Testkonto bei dem Web-Interface von Bitdefender GravityZone unter https:// gravityzone. bitdefender. com/ ein. Daraufhin erschien eine Willkommensseite, die uns erklärte, wie die Installation der Agenten-Software auf den Rechnern im Netz abläuft. Außerdem informiert sie darüber, wie Sicherheitsrichtlinien erstellt werden, wie die Benutzerkontenverwaltung funktioniert und wie sich Reports generieren lassen. Wir gingen zu diesem Zeitpunkt dazu über, die Endpoint Security Tools in unserem Netz zu verteilen.

Um diese Tools auf den Endpoints einzuspielen, ist es zunächst einmal erforderlich, passende Installationspakete zu erstellen. Dazu wechselten wir im Test nach “Netzwerk / Pakete” und fügten ein neues Paket für Windows-10- und Windows-11-Clients hinzu. Bei der Definition der Pakete haben die zuständigen Mitarbeiter die Möglichkeit, diejenigen Module der Endpoint Security Tools auszuwählen, die auf

den jeweils betroffenen Endgeräten zum Einsatz kommen sollen. Dank des modularen Aufbaus der Tools besteht also die Option, für bestimmte Geräte oder auch Geräteklassen exakt angepasste Security-Tool-Konfigurationen einzurichten.



Die Konfigurationsseite der modular aufgebauten Endpoint Security Tools

Die Module der Endpoint Security Tools

Zu den Modulen, die ein Administrator auswählen kann, gehören unter anderem eine Anti-Malware-Funktion, eine Firewall, eine Advanced Threat Control, die eine Prozessanalyse durchführt und eine Network Protection, die auch eine Network-Attack-Defense-Funktion mitbringt. Dazu kommen noch ein EDR-Sensor (Endpoint Detection and Response) und Funktionen zum Patch Management, zum Integrity Monitoring (also zum Überwachen der Registry- und Dateiintegrität), zum Absichern von Containern, für die Verschlüsselung, zur Gerätesteuerung und Ähnlichem. Aktivieren die IT-Verantwortlichen das "Power User"-Feature, so ermöglichen sie damit den Endanwendern auf den betroffenen Rechnern, die einzelnen Funktionen der Client-Software direkt auf den Endpoints zu konfigurieren. Dazu benötigen sie aber einen, durch ein Passwort geschützten, Power-User-Account. Die Passwörter für diese Konten können über die Richtlinien gesetzt werden. Darüber hinaus existiert auch ein Exchange-Modul, das sich in den Microsoft-Exchange-Transport-Dienst integrieren kann und dann dazu in der Lage ist, die Postfächer zu scannen und zu filtern.

Unterschiedliche Scan-Modi für verschiedene Einsatzszenarien

Ebenfalls von Interesse bei der Konfiguration der Installationspakete für die Client-Systeme: die verschiedenen Scan Modi. Im automatischen Modus untersucht die Bitdefender-Software die Hardware der jeweiligen Zielsysteme und entscheidet anhand der vorhandenen Ressource – wie beispielsweise der Größe des Arbeitsspeichers – welcher Scan Modus zum Einsatz kommt. Bei Bedarf besteht aber auch die Option, den Modus fest vorzugeben. Beim "Lokalen Scan" sind alle Technologien direkt auf dem Endpoint installiert und alle Scans laufen auch direkt auf dem System ab.

Der "Hybrid Scan" eignet sich für Rechner mit beschränkten Ressourcen, wie beispielsweise Systeme aus der Zeit von Windows 7. In diesem Modus existieren immer noch lokale Scan Engines, diese kommen aber seltener zum Einsatz, da die Sicherheits-Software Hashes der auf dem Client vorhandenen Dateien an die Cloud sendet und von dieser, sofern die Hashes bekannt sind, Informationen darüber erhält, ob die Files infiziert wurden oder nicht. Deswegen ist es im hybriden Modus nicht erforderlich, alle Dateien lokal zu scannen und es lassen sich laut Bitdefender 30 bis 40 Prozent Ressourcen einsparen.

Der "Central Scan" wurde ursprünglich für virtuelle Maschinen (VMs) entwickelt. Hier werden keine Scan Engines eingespielt, sondern lediglich ein Treiberpaket, das einen Dateisystemtreiber enthält. Dieser Treiber macht es möglich, jede geöffnete Datei auf einem zentralen Scan-Server zu überprüfen. Das führt zu einem minimalen lokalen Ressourcen-Verbrauch. Bitdefender empfiehlt in diesem Zusammen-

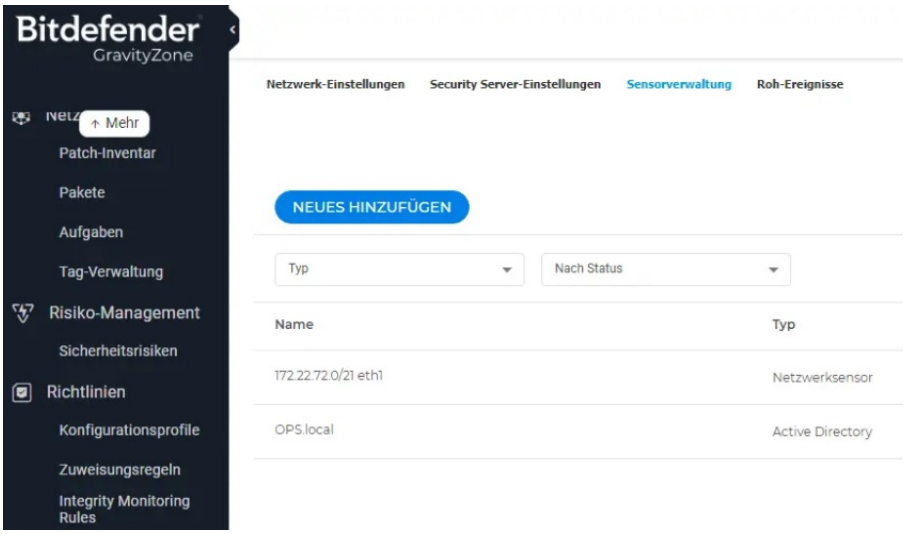
hang, etwa 200 Maschinen von einem Scan-Server absichern zu lassen. Die genannten Server sind übrigens nicht getrennt zu lizenzieren, deswegen kann jede IT-Abteilung frei entscheiden, wie viele davon sie – beispielsweise aus Redundanzgründen – einsetzen möchte.

Wollen die IT-Verantwortlichen den Scan Modus vorgeben, so können sie dies getrennt für Computer, VMs und Amazon EC2-Instanzen machen. Für die beiden letztgenannten Systemtypen gibt es sogar die Möglichkeit, eine Fallback-Option festzulegen, die aktiv wird, wenn der eigentlich vorgegebene Modus nicht funktioniert. Wurde beispielsweise ein Central Scan vorgegeben und es besteht keine Verbindung zu einem Scan-Server, so kann das System bei entsprechender Konfiguration automatisch auf einen lokalen Scan wechseln.

Im Test legten wir drei verschiedene Pakete an. Für Windows Clients aktivierten wir die Malware-Protection, die Advanced Threat Control, den erweiterten Exploit-Schutz, die Firewall, den Netzwerkschutz, das Integrity-Monitoring und den EDR-Sensor. Bei den Windows Servern ließen wir das Firewall-Modul beiseite und für Exchange-Server verwendeten wir die gleiche Konfiguration wie für Windows Server, aber mit aktiviertem Exchange-Modul.

Nach dem Abschluss der Konfiguration der Installationsdateien besteht die Möglichkeit, entweder das komplette Installationspaket für das jeweils gewünschte Betriebssystem herunterzuladen oder lediglich eine Download-Datei zu erzeugen, die auf dem jeweiligen Endpoint ausgeführt wird und dort die Setup-Routine herunterlädt und ausführt. Im Test setzten wir beide Methoden ein, dabei kam es zu keinen Problemen.

Insgesamt spielten wir die Lösung auf einem Server unter Windows Server 2019, der als Domänen-Controller zum Einsatz kam, einer VM unter Windows Server 2019 (ebenfalls ein Domänen-Controller), einer VM unter Windows Server 2016 mit Exchange 2016 CU23 und diversen Clients unter Windows 10 und 11 ein. Diese meldeten sich kurz nach der Installation bei dem Web-Interface und erschienen ohne weiteres Zutun von unserer Seite in der dortigen Netzwerkübersicht. Bei Bedarf gibt es übrigens auch die Möglichkeit, ferngesteuerte Installationen, beispielsweise über das Active Directory, durchzuführen.



Unsere Umgebung mit den beiden aktiven Zusatzsensoren

Das Aktivieren zusätzlicher Sensoren

Im letzten Schritt der Inbetriebnahme von GravityZone, aktivierten wir noch die genannten beiden Zusatzsensoren, um weitere Informationen über unsere Umgebung einbinden zu können. Zum einen verwendeten wir den Active-Directory-Sensor, um Login-Daten von den Rechnern im Netz zu erfassen, zum anderen nutzten wir den Netzwerk-Sensor, um die Datenübertragungen zwischen den Systemen im Auge zu behalten.

Um den Active-Directory-Sensor zu aktivieren, muss der zuständige Mitarbeiter nach "Konfiguration / Sensorverwaltung" wechseln und den genannten Sensor selektieren. Danach weist das System ihn darauf hin, dass die Endpoint Security Tools auf allen Domänencontrollern in der zu überwachenden Domäne laufen müssen und dass es erforderlich ist, die Gruppenrichtlinien so anzupassen, dass alle Anmeldungsereignisse überprüft werden. Wie das genau funktioniert, wird im Detail in der Dokumentation beschrieben, so dass wir an dieser Stelle nicht weiter darauf eingehen müssen. Anschließend wählen die Administratoren nur noch die Domäne mit den Servern aus, danach geht der Sensor in Betrieb. Der bereits beschriebene Netzwerksensor sammelt auch Informationen von Systemen, die nicht von GravityZone verwaltet

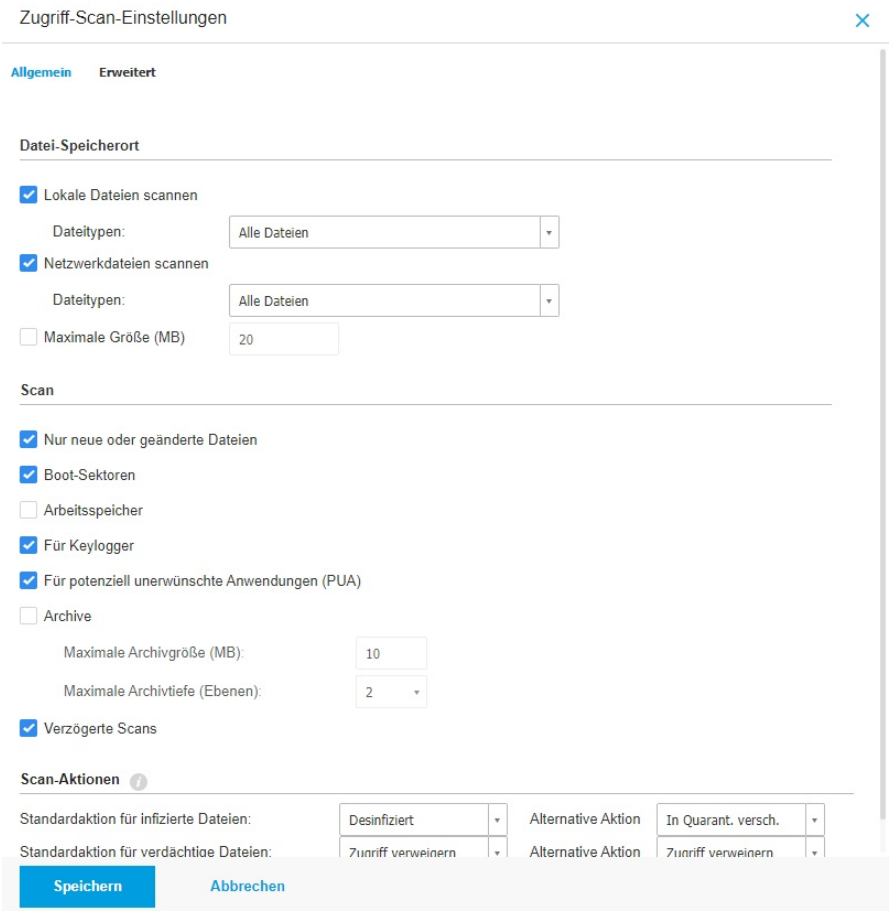
werden, wie Handys oder Druckern. Es lässt sich dann beispielsweise feststellen, von welcher IP-Adresse aus eine Malware ins Netz gelangen konnte. Im Test verwendeten wir eine VM für Vmware, die wir auf einem ESXi-Hypervisor in der Version 8.0a importierten. Dabei traten keine Probleme auf. Bei Bedarf steht auch eine Hyper-V-Version des Sensors zur Verfügung.

Um die Verbindung des Sensors zur Cloud herzustellen, müssen sich die Verantwortlichen nach dem Hochfahren des Systems lediglich mit den Standard-Credentials „root/sve“ auf der Console der VM anmelden und das Passwort ändern. Danach können sie das Skript „/opt/bitdefender/bin/sva_setup.sh“ aufrufen, die Netzwerk- und Proxy-Konfiguration durchführen und auswählen, mit welcher Cloud-Instanz von Gravity-Zone sich der Sensor verbinden soll. Danach ist es nur noch erforderlich, einen „Company hash“ einzutragen, der ich in der Lizenzübersicht des GravityZone-Web-Interfaces findet. Dann nimmt die VM die Verbindung zur Cloud auf und erscheint in der Übersicht der vorhandenen Komponenten. Im Test ergaben sich auch dabei keinerlei Schwierigkeiten. Die VM setzt übrigens auf Ubuntu-Linux 20.04.5 LTS auf.

Die Arbeit im laufenden Betrieb

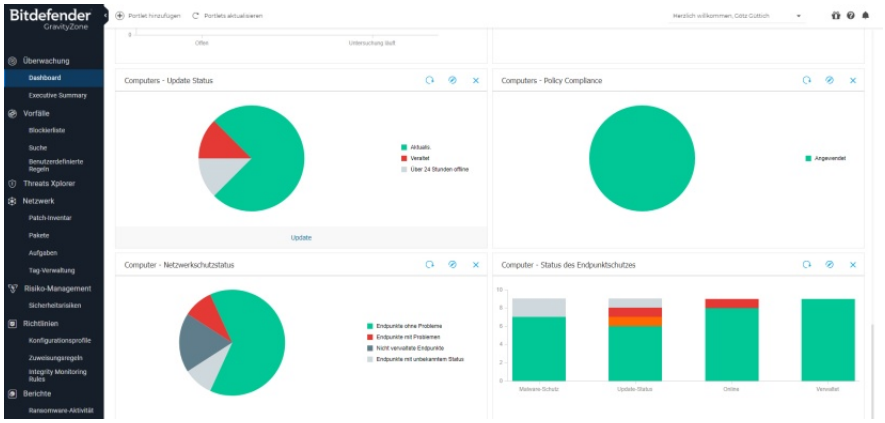
Nachdem wir die Endpoint Security Tools auf allen unseren Testrechnern installiert und die Zusatzsensoren in Betrieb genommen hatten, erstellten wir zunächst einmal eine Richtlinie für GravityZone. Dieser Schritt ist nicht unbedingt erforderlich, da die Lösung bereits mit einer Standardrichtlinie mit empfohlenen Einstellungen kommt, wir wollten uns aber im Detail mit dem Leistungsumfang des Produkts auseinandersetzen. Dabei legten wir unter anderem fest, wie oft die Lösung nach Updates suchen sollte, ob eine Überprüfung von USB-Speichergeräten und optischen Medien gewünscht war und wie die Regeln für die Firewall aussahen. Darüber hinaus sind die Administratoren bei der Richtlinienkonfiguration auch dazu in der Lage festzulegen, welche Dateien in Scan-Vorgänge eingebunden werden, ob der Netzwerkschutz HTTPS- und RDP-Übertragungen überwacht und wie Patch Management, Verschlüsselung und Integrity Monitoring arbeiten. Sobald eine Richtlinie fertig konfiguriert wurde, lässt sie sich unter “Netzwerk” einem oder mehreren Geräten zuweisen.

Interessant ist in diesem Zusammenhang noch die Funktion “Ransomware Mitigation”, die sich bei den Antimalware-Einstellungen der Richtlinienkonfiguration findet und die in der Standardrichtlinie nicht aktiviert wurde. Diese verhindert Datenverluste durch Ransomware auch dann, wenn die betroffene Malware nicht erkannt wurde. Das funktioniert folgendermaßen: Das System erkennt laufende Verschlüsselungsvorgänge und legt bei suspekten Aktionen automatisch Backup-Kopien von den verschlüsselten Dateien an. Verschlüsselungsvorgänge von legitimen Anwendungen werden dabei nicht beeinträchtigt. Stuft Bitdefender den Vorgang aber als suspekt ein, so blockiert die Lösung die Aktion automatisch nach 20 bis 30 Dateien. Diese lassen sich dann aus dem Backup wieder herstellen.



Die Scan-Einstellungen in der Richtliniendefinition

Nachdem in unserem Netz der erste Scan-Vorgang durchgelaufen war und GravityZone die oben genannten Probleme gefunden und beseitigt hatte, schauten wir uns zunächst einmal im Detail an, was die Bitdefender-Lösung zu bemängeln hatte und welche Maßnahmen ergriffen wurden. Dazu wechselten wir nach “Vorfälle”. Dort gibt es insgesamt drei Reiter. Unter “Gefundene Bedrohungen” sortiert



Das Dashboard ist genau an die Anforderungen der Administratoren anpassbar

Bitdefender alle Malware-Funde ein. Hierbei ist sich die Lösung sicher, dass es sich wirklich um Malware handelt. Diese Vorfälle können die zuständigen Mitarbeiter zu Analysezwecken unter die Lupe nehmen, sie wurden aber von der Security-Lösung bereits abgeschlossen, so dass keine Gefahr mehr von ihnen ausgeht. Hier sind also von Seiten der Administratoren keine Aktionen erforderlich.

Die Darstellung der Sicherheitsvorfälle hilft bei der Analyse

Interessant ist aber die Art und Weise, wie die einzelnen Vorfälle dargestellt werden. Es gibt – wie erwähnt – sowohl eine grafische Darstellung, die in Diagrammform zeigt, was genau in welcher Reihenfolge ablief, als auch eine Ereignisanzeige in Listenform. Nehmen wir an dieser Stelle als Beispiel einen Virenfund auf dem Testsystem “PC08”. Hier wurde der Prozess “winlogon.exe” als Ursprung des Prozesses erkannt und der Prozess “userinit.exe” als beteiligt markiert. Der nächste Prozess, der mit der Aktion zu tun hatte, war “explorer.exe”. Dieser Prozess interagierte mit einer ganzen Zahl anderer Prozesse, von denen die meisten unproblematisch waren, wie “prtgdesktop.exe”, “nextcloud.exe”, oder auch “onedrive.exe”. Diese Prozesse sind dann auch in dem Diagramm grau oder gelb markiert. Gelb bedeutet lediglich, dass sie als verdächtig markiert wurden, da sie sich in einem verdächtigen Prozessbaum befinden. Blau werden übrigens Einträge gekennzeichnet, die das System für wichtig hält.

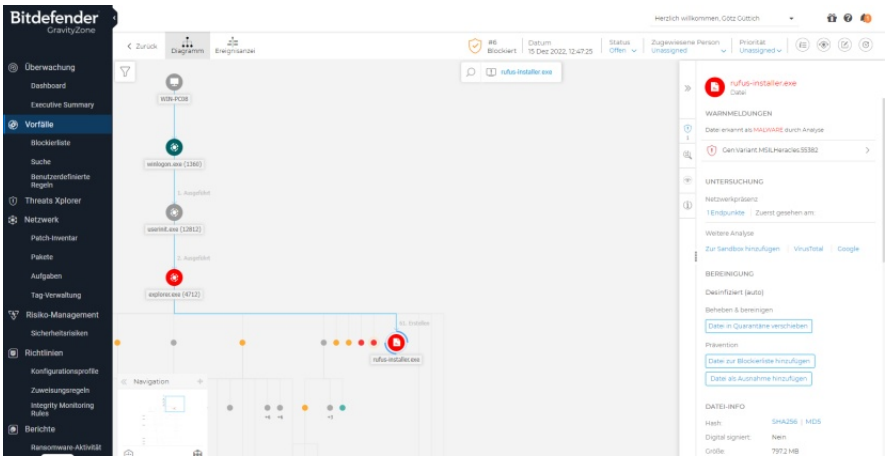
Jetzt aber zurück zu “explorer.exe”. Dieser Prozess hatte auch mit “rufus-installer.exe” zu tun und diese Datei enthielt die Malware “Gen: Variant. MSIL-Heracles. 55382”. Deswegen wurde die fragwürdige Datei in die Quarantäne verschoben. Das Diagramm visualisiert also auf anschauliche Weise, wie die einzelnen Faktoren zusammenhängen und welche Aktionen durchgeführt wurden.

Die Ereignisanzeige umfasst im Gegensatz dazu eine Liste, in der die einzelnen Aktionen nacheinander aufgeführt sind. Diese umfasst Verbindungsaufnahmen, das Schreiben von Registry-Einträgen, Schreibvorgänge bei Dateien, Aktionen bei denen Dateinamen umbenannt wurden (beispielsweise mit Änderung der Dateinamenserweiterung) und vieles mehr. Hier lassen sich folglich tiefgehende Analysen anstellen, die durch umfassende Filterfunktionen unterstützt werden.

Ein weiteres Beispiel: Ransomware

Neben dem Reiter “Gefundene Bedrohungen” haben die IT-Mitarbeiter Zugriff auf die “Endpunktvorfälle”. Diese umfassen Einträge, die bearbeitet werden müssen. Spielen wir hier an dieser Stelle einmal beispielhaft durch, wie ein laufender Ransomware-Angriff im Web-Interface präsentiert würde. Damit so etwas in der Praxis auch an dieser Stelle erscheint, müssen die Verantwortlichen allerdings eine unbekannte Ransomware verwenden oder GravityZone zuerst in einen Monitoring-only-Modus versetzen, da das System den Angriff sonst sofort unterbinden würde. Nun aber zum Beispiel: Geht auf einem Rechner im Netz eine E-Mail mit einer Word-Datei mit Makros, die schädliche Aktionen durchführen, als Anhang ein und öffnet ein Anwender diese, so werden diese Makros logischerweise aktiv. GravityZone stellt nun die ablaufenden Aktionen wieder in der zuvor geschilderten Form als Diagramm und Ereignisanzeige dar. Über das Diagramm könnte man beispielsweise sehen, dass die Makros eine Powershell aufgerufen haben, die wiederum zu Einsatz kam,

um von einer dubiosen Webseite eine Datei namens “acro32.exe” herunterzuladen. Diese wiederum eignete sich nicht für das Anzeigen von PDF-Dateien, sondern verschlüsselte auf dem Endpoint diverse Excel-Files. Ein solcher Angriff wird allerdings – wie bereits gesagt – nur dann bis zum letzten Schritt durchlaufen und dementsprechend geloggt werden, wenn die Administratoren die Bitdefender-Software zu Testzwecken im Reporting-Modus



Die Diagrammübersicht stellt die Sicherheitsereignisse plastisch dar. Rote Punkte symbolisieren Gefahren, gelbe stehen mit Gefahren in einem Zusammenhang. Graue Punkte dienen der Information und blaue sind nach Ansicht des Systems wichtig.

betreiben. Ansonsten würden die Makros bereits zu Beginn der Aktion gestoppt und der ganze Vorgang wäre abgeschlossen und von GravityZone unter “Gefundene Bedrohungen” einsortiert worden.

Die zur Verfügung stehenden Gegenmaßnahmen

Hat ein Administrator mit einem Angriff zu tun, den GravityZone nicht alleine beseitigen kann, so gibt es die Option, die betroffene Maschine zu isolieren, über das Patch-Management-Modul Patches einzuspielen oder über eine Remote Shell auf das System zuzugreifen um das Problem zu lösen. Außerdem gibt es auch die Möglichkeit, verdächtige Dateien, wie das eben genannte Word-Dokument in die Bitdefender-Sandbox oder zu Virustotal hochzuladen und dort überprüfen zu lassen.

Alternativ können die Verantwortlichen auch per Klick auf Google nach dem Hash der Datei suchen. Zusätzlich sind die IT-Mitarbeiter auch dazu in der Lage, die Datei manuell in Quarantäne zu schicken oder sie zu einer Blockliste hinzuzufügen. Diese Blockliste arbeitet mit Datei-Hashes und blockiert die Datei auf allen Rechnern, die zu der Umgebung gehören. Es gibt übrigens noch eine Option, um herauszufinden, ob sich eine Malware im Netz verbreitet hat: Dazu können die zuständigen Mitarbeiter aus der Diagrammübersicht den Hash der Schaddatei kopieren und diesen dann in der Netzwerkübersicht auf beliebigen Rechnern im Netz suchen. Dazu steht extra eine Aufgabe namens “Nach IOCs suchen” (Indicator of Compromise) zur Verfügung. Auf die gleiche Art und Weise lassen sich auch Suchen nach Datei- und Prozessnamen, Registrierungsschlüsseln und Ähnlichem erstellen.

Von EDR zu XDR

Der dritte Reiter unter „Vorfälle“ nennt sich “Erweiterte Vorfälle” und umfasst Ereignisse, die sich auf mehrere Rechner im Netz beziehen, beispielsweise durch laterale Bewegungen. Ein solcher Vorfall könnte beispielsweise wieder mit einer E-Mail beginnen, die auf einem Rechner ankommt. Danach könnte der Urheber der in der Mail vorhandenen Malware einen Exploit benutzen, um Zugriff auf einen Domänencontroller zu erhalten und anschließend mittels Brute-Force-Angriff die Zugangsdaten eines Benutzers stehlen. Daraufhin wäre er dann in der Lage, mit Hilfe der Powershell Daten auf Systeme im Internet hochzuladen und so kritische Informationen abzugreifen. Eine Zusammenfassung eines solchen Vorgangs mit den wichtigsten Schritten findet sich im Konfigurations-Interface in der Übersicht des zum jeweiligen Ereignis gehörenden Eintrags.

Weitergehende Informationen stellt GravityZone wieder in der bekannten Diagrammanzeige dar. Diese ist sehr detailliert und zeigt genau, welcher User wann die eingehende E-Mail erhalten hat, auf welchen Rechnern Login-Vorgänge stattgefunden haben, und so weiter. Um die Übersichtlichkeit zu verbessen, lässt sich diese Anzeige auch einschränken, so dass das System beispielsweise nur laterale Bewegungen darstellt. Damit das alles funktioniert, reichen allerdings die Security-Werkzeuge auf den Endpoints nicht aus, es müssen weitere Sensoren aktiviert werden, beispielsweise zum Überwachen der Mail-Server, um zu erkennen, welche Mail der Ursprung des Vorfalls war. Außerdem muss auch der Active-Directory-Sensor

laufen, der im Auge behält, wer sich wann auf welchem Rechner angemeldet hat. Um den laufenden Angriff abzuwehren, stehen den Administratoren dann wieder verschiedene Aktionen zur Verfügung, wie zum Beispiel das Isolieren von Rechnern, das Zurücksetzen von Zugangsdaten und das Löschen von E-Mails.

Die Überwachung von Exchange-Servern

Gehen wir zum Abschluss des Tests noch kurz auf die Funktion zum Überwachen von Exchange-Servern ein. Wie bereits angesprochen, müssen die Administratoren dieses Feature bereits bei der Konfiguration des Setup-Pakets aktivieren und die Endpoint Security Tools dann mit dieser aktivierten Funktion auf dem Exchange Server einspielen. Die Konfiguration der Funktion erfolgt dann über die Richtlinien unter "Exchange-Schutz". Hier geben die Verantwortlichen an, wie lang das System Dateien in der Quarantäne vorhält und aktivieren den Spoofing-Schutz. Außerdem lassen sich Malware-Filter setzen, die festlegen, ob die Scans für aus- oder eingehende Mails (oder beides) durchgeführt werden, welche Dateitypen zu scannen sind (Anwendungen, bestimmte Endungen und so weiter) und welche Aktionen GravityZone durchführen soll (Desinfizieren, Löschen, Quarantäne und Ähnliches). Auch hier gibt es wieder die Option, alternative Aktionen zu definieren, die ablaufen, wenn die eigentliche Aktion nicht funktioniert. Abgesehen davon gehören noch Antispam-Regeln zum Leistungsumfang des Exchange-Schutzes. Bei den entsprechenden Einstellungen geben die Administratoren an, bestimmte Inhalte zu filtern (kyrillisch, asiatisch, sexuell, etc.) und legen unter anderem auch fest, wie aggressiv die Funktion arbeiten soll (aggressiv, normal oder tolerant). An Aktionen gibt es dann die Möglichkeiten "zustellen", "im Betreff markieren", "umleiten", "ablehnen" und "Quarantäne".

Zu guter Letzt bietet der Exchange-Schutz noch eine Inhaltssteuerung und eine Anhangsfilterung an. Erstere ermöglicht es, bestimmte Betreffs und Nachrichteninhalte zu filtern und die betroffenen Mails dann abzulehnen, zuzustellen und so weiter. Mit letzterer sind Administratoren dazu in der Lage, Anhänge nach Kriterien wie "ausführbare Dateien", "Bilder", Multimedia", "Archive", "Tabellenkalkulationsdatei", "Präsentationen" und "Dokumente" zu filtern. Bei Bedarf lassen sich für die Filterfunktion auch benutzerdefinierte Endungen angeben. Darüber hinaus steht auch eine "Erkennung des echten Dateityps" anhand von Signaturen zur Verfügung, damit die Anwender den Filter nicht einfach durch das Ändern der Dateiendung umgehen können. Es ist auch möglich, gefundene Archive direkt zu scannen. Erkennen die Filter ungewünschte Inhalte, kommen auch hier wieder Aktionen wie "Löschen", "Zustellen", "Quarantäne" und so weiter zum Einsatz. Im Test funktionierten die Exchange-Schutzfunktionen einwandfrei.

Zusammenfassung und Fazit

Bitdefender bietet mit GravityZone Business Security Enterprise eine Lösung an, die IT-Administratoren dabei hilft, einen vollständigen Einblick in den Sicherheitsstatus ihrer Netzwerke zu erhalten. Das System ist nicht nur dazu in der Lage, einen Großteil der Sicherheitsvorfälle selbst zu lösen, sondern gibt den IT-Verantwortlichen auch umfassende Informationen in die Hand, die klären, was genau wann wie und wo geschehen ist. Darüber hinaus existiert auch eine große Auswahl an Gegenmaßnahmen, mit denen die zuständigen Mitarbeiter Angriffe abwehren können.

Das System ist genau an die jeweiligen Anforderungen anpassbar. So besteht beispielsweise die Möglichkeit, die Endpoint Security Tools dank ihres modularen Aufbaus so zu gestalten, dass sie exakt die Funktionen mitbringen, die auf den jeweiligen Endpoint-Typen erforderlich sind. Aber auch das Dashboard im Konfigurations-Interface der Lösung kann speziell an die Bedürfnisse der IT-Abteilung angepasst werden, so dass es immer die Daten präsentiert, die im jeweiligen Unternehmensnetz am wichtigsten sind. Der Funktionsumfang von GravityZone ist sehr groß, so dass wir in diesem Test nicht auf alle Features der Lösung eingehen konnten. So existiert beispielsweise eine „Executive Summary", die eine Darstellung des Sicherheitsstatus bietet, die auch für Nichtspezialisten geeignet ist. Zu den weiteren Funktionen, die von Interesse sind, gehört zudem ein Risikomanagement, das die Konfiguration der Rechner im Netz, die App-Schwachstellen, das Verhalten der Nutzer und Ähnliches analysiert und Vorschläge dazu macht, wie sich das Sicherheitsniveau verbessern lässt. Unter dem Strich ist GravityZone eine extrem leistungsfähige Lösung mit vielen sinnvollen Funktionen. Wir verleihen der Lösung deshalb das Attribut „IT-Testlab Tested and Recommended".