07 | 22 Sonderdruck für WatchGuard Technologies

IT Administrator
Das Magazin für professionelle System- und Netzwerkadministration

WatchGuard Passport

www.it-administrator.de

WatchGuard Passport

Umfassender Reiseschutz

von Dr. Christian Knermann

Mit Passport schnürt WatchGuard ein aus drei Modulen bestehendes Sicherheitspaket für mobile Clientrechner und Benutzer. Zu einer fortgeschrittenen Abwehr von Malware und Exploits gesellen sich die Absicherung von DNS-Anfragen sowie ein System zur systemübergreifenden Multifaktor-Authentifizierung. IT-Administrator hat die umfangreiche Suite in der Praxis ausprobiert.

Der Hersteller WatchGuard hat sich vor allem mit Angeboten rund um die Netzwerksicherheit einen Namen gemacht. Den Trends zu Virtualisierung und Cloud folgend bietet das Unternehmen die hauseigenen Firebox-Firewalls sowohl als physische Appliances sowie in Form von virtuellen Maschinen an. Diese Art der Absicherung von Netzwerken wird zwar mittelfristig weiter eine wichtige Rolle spielen, doch nimmt die Bedeutung des klassischen Perimeters mit dem Trend zu immer mobilerem Arbeiten ab. An die Stelle der früheren Unterscheidung zwischen Drinnen und Draußen, zwischen Gut und Böse, tritt das Prinzip von Zero Trust, das grundsätzlich alle Clients und Benutzerkonten als potenziell kompromittiert annimmt.

WatchGuard hat das eigene Produktangebot darauf ausgerichtet und mit Passport ein Paket für mobile Clients und Benutzer geschnürt, das diese besonders dann absichern soll, wenn sie sich außerhalb eines internen Unternehmensnetzes bewegen. Passport umfasst drei optionale Module, die sich nach Belieben miteinander kombinieren lassen.

Abwehr von Malware und Exploits

WatchGuard EPDR (Endpoint Protection, Detection & Response) adressiert die Abwehr von Malware sowie fortgeschrittenen Angriffstechniken. Es handelt sich dabei um einen alten Bekannten, denn WatchGuard hat dieses Modul nicht neu entwickelt, sondern den früheren Anbieter Panda Security mit dessen Flaggschiff "Panda Adaptive Defense 360" (AD360) übernommen.

WatchGuard EPP (Endpoint Protection Plattform), vormals "Panda Adaptive Defense", fungiert als klassischer Virenscanner mit Signaturen und Heuristiken. WatchGuard EDR (Endpoint Detection & Response) bietet zusätzlich die cloudbasierte Abwehr fortschrittlicher Attacken wie Advanced Persistent Threats (APT), Exploits und dateilose Angriffe. Wer als Grundschutz einem anderweitigen klassischen Virenscanner vertraut, kann EDR zusätzlich dazu einsetzen. WatchGuard EPDR bietet den kompletten Schutz aus einer Hand und das plattformübergreifend für Windows, theoretisch sogar noch abwärtskompatibel bis XP, macOS, Linux sowie Android. Windows und macOS dürfen sowohl auf Intel-kompatiblen als auch auf ARM-Prozessoren laufen.

Zusätzlich zum Malwareschutz bietet WatchGuard mehrere Untermodule für EPDR an, darunter Patchmanagement, Laufwerksverschlüsselung sowie erweitertes Reporting und Anbindung an SIEM-Systeme. Welche Funktionen auf welcher Plattform zur Verfügung stehen, schlüsselt WatchGuard in einem separaten Datenblatt auf, wobei EPDR für Windows den größten Funktionsumfang bietet.

DNSWatchGO als zweites Modul von Passport ergänzt den Schutz vor DNS-basierten Phishing- und Malwareangriffen. Als DNSWatch zählt diese Option zu den ursprünglichen Funktionen der Firewalls aus der Firebox-Familie. Mit DNSWatchGO bringt WatchGuard einen Softwareclient, der Systeme auch außerhalb von per Firebox gesicherten Netzen schützt, aktuell allerdings nur für Windows und als Erweiterung für Chrome OS.

Schließlich schützt das dritte Modul AuthPoint Benutzerkonten mithilfe von Multifaktor-Authentifizierung (MFA). AuthPoint integriert herstellerübergreifend sämtliche Dienste lokal und in Clouds, sofern sich diese auf RADIUS- oder SAML-Authentifizierung verstehen, und klinkt sich auch in die lokalen Anmeldeprozesse von Windows sowie macOS ein.

Der Hersteller lizenziert die Module wahlweise einzeln oder als günstigeres Gesamtpaket jeweils pro Benutzer. WatchGuard vertreibt die Produkte indirekt über Distributoren und Reseller, die auf Anfrage verschiedene Modelle anbieten – klassische Kauf-Lizenzen mit jährlicher Wartung oder Subskription (Mietlizenz).

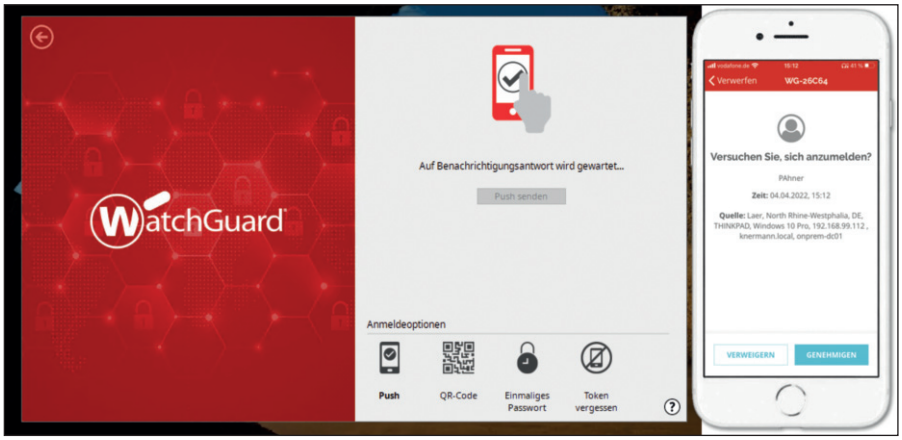

Bild 1: WatchGuard AuthPoint erweitert den Anmeldeprozess von Windows um MFA.

Klicken durch drei separate Webportale

Wir registrierten uns auf der Webseite des Herstellers für einen WatchGuard-Account. Dabei durften wir wählen, in welcher geografischen Region unsere Daten liegen sollen. Wir entschieden uns hier für die EU. Anschließend forderten wir jeweils 30 Tage gültige Trial-Lizenzen für die drei Passport-Module an, die sich nach Bedarf um weitere 30 Tage verlängern ließen.

Zur Konfiguration benötigten wir drei separate Webportale, da die Funktionen von Passport noch nicht vollständig unter einer Haube integriert sind. EPDR und AuthPoint erreichten wir unter der Adresse "cloud.watchguard.com", von dort gelangten wir per Single Sign-on (SSO) in ein separates Webfrontend für die Malwareabwehr, das noch unter der Domain von Panda Security firmierte. DNSWatchGO konfigurierten wir mittels einer separaten Oberfläche unter "dns-watch.watchguard.com".

Flexible Richtlinien für MFA

Um uns mit den Funktionen von AuthPoint vertraut zu machen, folgten wir zunächst der Schnellstartanleitung aus der Onlinedokumentation des Herstellers. Die sieht den simpelsten Fall vor, nämlich die Absicherung der Anmeldung am Identity-Provider-(IDP)-Portal des Herstellers selbst. Dazu navigierten wir im Webportal in den Bereich "Configure / Services / AuthPoint".

WatchGuard verfolgt hier das Prinzip, Benutzer in Gruppen zusammenzufassen und diese über Authentication Policies mit Ressourcen zu verknüpfen, deren Login AuthPoint dann per MFA schützt. Entsprechend wählten wir aus dem Untermenü den Punkt "Configuration / Resources" und fügten das IDP-Portal als neue Ressource hinzu. Weiterhin unterstützt WatchGuard als Ressourcen die "Logon App", auf die wir gleich zurückkommen werden, die hauseigenen Firebox-Firewalls sowie generische RADIUS-Clients und SAML-Ressourcen. Zudem konnten wir Active Directory Federation Services (ADFS), Microsofts Remotedesktopdienste-Webaccess sowie REST-APIs anbinden.

Nun legten wir eine Gruppe an, gefolgt von einer Authentication Policy. Dabei durften wir aus vier Optionen wählen, welche Arten der Authentifizierung die Richtlinie unterstützen soll. Neben Passwörtern sind dies zusätzlich Push-Benachrichtigungen, QR-Codes sowie One-Time-Passwords (OTP). Eine Richtlinie bindet optional "Policy Objects" ein. Dies sind Bausteine für zusätzliche Sicherheitsmerkmale, die wir vorab unter dem Menüpunkt "Configuration / Policy Objects" konfigurierten. Objekte vom Typ "Geofence" beschränken den Login auf ein oder mehrere Länder, "Network Locations" auf frei definierbare IPv4-Adressbereiche und Objekte vom Typ "Time Schedule" lassen die Anmeldung nur in vorgegebenen Zeiträumen zu.

Zu guter Letzt fügten wir im Bereich "Configuration / Users" einen Benutzer hinzu. Es handelte sich in diesem Fall um ein Benutzerkonto, das nur in der Cloud von WatchGuard existiert und über eine gültige E-Mail-Adresse verfügen muss. An diese schickte WatchGuard mehrere

WatchGuard Passport

Produkt
Cloudbasierte Security-Suite für mobile Clients und User.

Hersteller
WatchGuard Technologies, Inc.
www.watchguard.com/de/wgrd-products/watchguard-passport

Preise
Exemplarisch für kleine bis mittlere Unternehmen mit 101-250 Benutzern kostet das Komplettpaket von WatchGuard Passport mit allen drei Modulen 195 Euro pro Benutzer für drei Jahre.

Systemvoraussetzungen
- AuthPoint: Für die Logon App Windows 8.1 oder 10, Windows Server 2012 R2 bis 2022, macOS 10.11 bis 12.x; Für das Gateway Windows Server 2012 R2 bis 2022, Amazon Corretto 8 bis 15 oder Oracle JRE 8 (Update 162) und für die Mobile App Apple i(Pad)OS oder Google Android.
- DNSWatchGO: Windows, Chrome OS
- EPDR: Windows XP SP3 bis 11, Windows Server 2003 bis 2022, macOS 10.10 bis 12.x sowie zahlreiche Linux-Distributionen, darunter Ubuntu ab 14.04 LTS, Fedora ab 23, RedHat / CentOS ab 6.0, Android 4 bis 12.

Technische Daten
www.it-administrator.de/downloads/datenblaetter

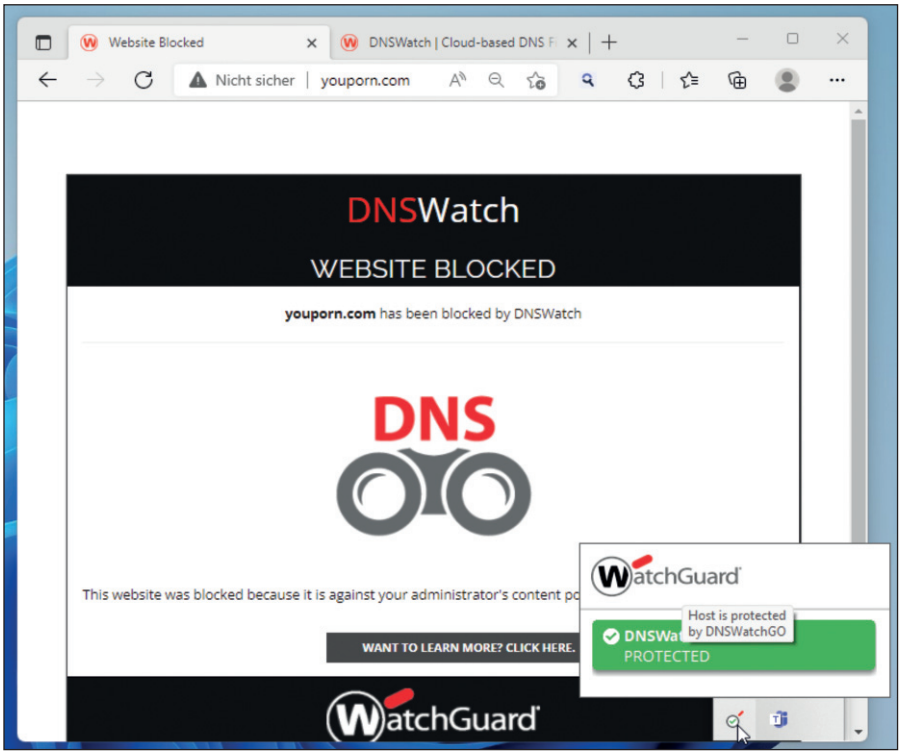

Bild 2: DNSWatchGO blockiert unerwünschte Webseiten bereits auf DNS-Ebene.

Nachrichten, mit deren Hilfe wir ein initiales Passwort sowie einen MFA-Token konfigurieren konnten. Dazu leitete uns WatchGuard zur Installation der AuthPoint-App, die in den App-Stores von Apple und Google verfügbar ist. Mithilfe eines QR-Codes gelang die Einrichtung des Tokens komplikationslos. Bei der anschließenden Anmeldung am IDP-Portal generierte die AuthPoint-App auf unserem mobilen Begleiter automatisch eine Push-Benachrichtigung, mit der wir die Authentifizierung bestätigten.

AD anbinden nur mit E-Mail-Adresse

Nun widmeten wir uns einem praxisrelevanteren Anwendungsfall, nämlich der Synchronisation von Benutzerkonten aus unserem Active Directory (AD) sowie der Absicherung des Logins an unseren Windows-Clients mithilfe der WatchGuard-Logon-App. Dazu richteten wir im ersten Schritt unter "Configuration / External Identities" den Verzeichnisdienst ein. WatchGuard unterscheidet hier zwei mögliche Quellen, entweder ein Azure AD oder eine generische LDAP-Quelle, die wir für unser lokales AD verwendeten.

Das Webfrontend verlangte nach den üblichen Parametern für eine solche Verbindung, einer Suchbasis in LDAP-Syntax sowie einem Systemkonto zum Zugriff auf das Verzeichnis. Als Intervall bot das Webfrontend wahlweise 15 oder 30 Minuten sowie alternativ eine, drei, sechs, zwölf oder 24 Stunden an. Wir beließen es beim Standardwert von einer Stunde und konfigurierten unsere Domain Controller (DC) zur unverschlüsselten LDAP-Synchronisation. Im produktiven Einsatz sollte LDAPS zum Einsatz kommen und zwecks Redundanz mehr als ein DC. Beides beherrscht AuthPoint.

Doch wie finden nun WatchGuard-Cloud und lokales AD zueinander? Hierzu benötigten wir noch ein Gateway, das wir unter "Configuration / Gateway" definierten. Dieses bildet die Brücke zu Authentifizierungsdiensten der Typen RADIUS, ADFS und LDAP. In unserem Fall wählten wir lediglich die zuvor konfigurierte LDAP-Verbindung zu unserem AD aus. Das Gateway erschien daraufhin in der Übersicht als noch nicht installiert. Wir erzeugten einen Registrierungsschlüssel und luden dann aus dem Bereich "General / Downloads" das Installationspaket für das Gateway herunter, das Windows Server 2012 R2 bis hin zur aktuellen Version 2022 unterstützt, als Voraussetzung aber zusätzlich eine Java-Runtime benötigt.

WatchGuard empfiehlt die Verwendung des Pakets "Amazon Corretto 11", das wir direkt vom Hersteller bezogen. Alternativ funktioniert auch das "Oracle Java Runtime Environment" (JRE). Auf unserem DC installierten wir Corretto, gefolgt vom MSI-Paket des Gateways. Das verlangte nach dem Registrierungsschlüssel und nahm daraufhin automatisch Verbindung zur WatchGuard-Cloud auf. Im Webfrontend wechselte der Status entsprechend zu "Connected".

In den Eigenschaften der Verbindung zu unserem AD konfigurierten wir einen "Group Sync", also die Abbildung einer Gruppe aus unserem internen AD auf eine Gruppe in AuthPoint, die wir zuvor angelegt hatten. Per "Advanced Query" unterstützt AuthPoint alternativ frei definierbare LDAP-Abfragen zur Auswahl der zu synchronisierenden Benutzer. Sobald wir dann mittels "Start Synchronization" den Abgleich manuell gestartet hatten, erschienen unter "Configuration / Users" die Benutzer aus unserem AD.

Das traf allerdings nur auf diejenigen Benutzer zu, deren E-Mail-Attribut jeweils mit einer extern erreichbaren Adresse belegt war. Benutzer ohne E-Mail-Adresse oder solche mit einer Adresse der Form "user@domain.local" synchronisiert WatchGuard nicht, denn eine gültige E-Mail-Adresse ist Voraussetzung für die Konfiguration von MFA. Im Zuge der Synchronisation schickte AuthPoint den jeweiligen Benutzern die Hinweise zur Einrichtung von MFA per E-Mail.

Schutz für lokale Anmeldungen

Im nächsten Schritt wechselten wir zu den Ressourcen, wo wir ein neues Objekt vom Typ "Logon App" hinzufügten. Hierbei aktivierten wir den Schalter "Allow specific users to log in without MFA". Daraufhin konnten wir per Freitext einen oder mehrere Benutzernamen definieren, die sich ohne MFA anmelden dürfen. Es empfiehlt sich, hier mindestens einen Administrator als "Break-Glass"-Account zu hinterlegen, falls die Anmeldung per MFA nicht funktionieren sollte. Sobald wir die Ressource konfiguriert hatten, bot uns das Webfrontend die Datei "wlconfig.cfg" zum Download an. Diese benötigten wir,

um die Logon-App bei ihrer Installation zu parametrisieren.

Zuvor erzeugten wir aber noch eine Authentication Policy, mit der wir die Gruppe unserer aus dem AD synchronisierten User und die Ressource verknüpften. Zu guter Letzt luden wir dann die Logon-App als MSI-Paket aus dem Downloadbereich herunter und installierten sie auf unseren Windows-Clients und -Servern. AuthPoint unterstützt weiterhin macOS. Bei der Installation verlangte die Setuproutine jeweils nach der "wlconfig.cfg". WatchGuard unterstützt auch die unbeaufsichtigte Installation mittels "msiexec" und Übergabe der Konfigurationsdatei per Kommandozeilen-Parameter.

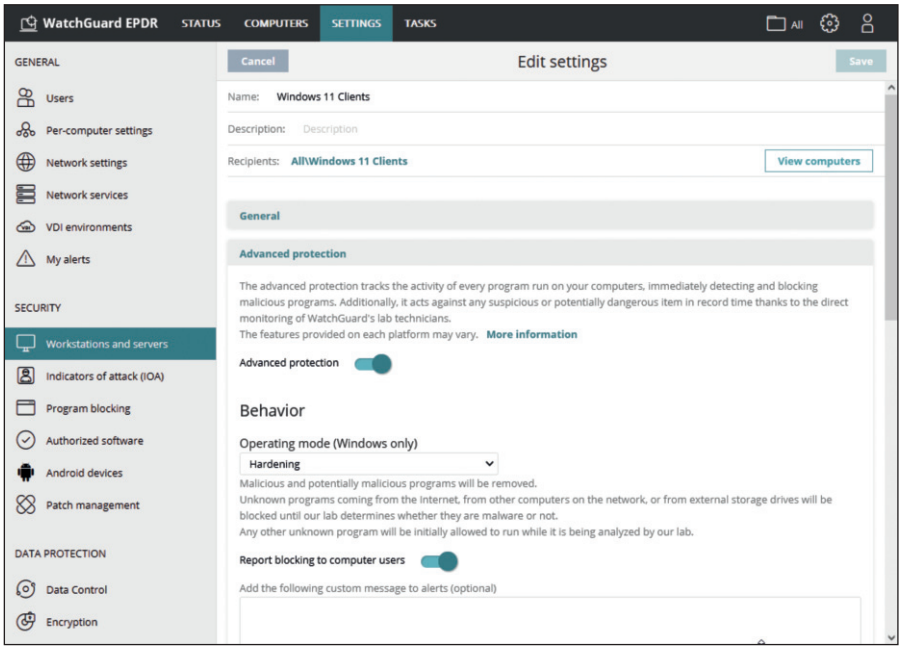

Bild 3: WatchGuard EPDR überprüft ausführbare Dateien mithilfe eines hauseigenen Clouddiensts.

Die Logon-App klinkte sich anschließend in den lokalen Anmeldeprozess ein. Nachdem wir Benutzer und Passwort eingegeben hatten, erschien ein weiterer Dialog von AuthPoint, der nach einem zweiten Faktor verlangte, und wir mussten die Anmeldung mithilfe der mobilen App bestätigen (Bild 1). Das funktionierte tadellos lokal an der Konsole unserer Test-Systeme sowie auch remote per RDP und über die verschiedenen angebotenen Verfahren. So konnten wir die Push-Benachrichtigung der Smartphone-App nutzen, alternativ einen vom Client-Computer angezeigten QR-Code scannen oder das in der App angezeigte sechsstellige OTP eingeben. Die Variante per QR-Code funktioniert sogar komplett offline, etwa im Flugzeug.

Auch die Fälle, dass ein Benutzer seinen mobilen Begleiter mit der AuthPoint-App verliert oder temporär keinen Zugriff darauf hat, berücksichtigt WatchGuard. Wir konnten im Anmeldedialog die Option "Token vergessen" nutzen, um ein Challenge-Response-Verfahren zu starten. Dabei generiert WatchGuard einen Activation Code, den ein Administrator im Webfrontend verifizieren und einen einmalig gültigen Freischalt-Code für den betroffenen Benutzer generieren kann.

Praktische Mobil-App

Die mobile App wusste weiterhin mit zusätzlicher Sicherheit zu überzeugen. So konnten wir einzelne Token per PIN sichern. Dabei generierte die App jeweils einen PUK-Code für den Fall einer vergessenen PIN. Zudem bot die App an, statt PIN die Touch-ID des mobilen Geräts zu verwenden, und unterstützte auch bei der Migration aller Token auf ein neues Mobilgerät. Neben den in AuthPoint definierten Anmeldeverfahren integriert die App auch TOTPs von Drittanbietern und dient so als Alternative zu anderweitigen Authenticator-Apps.

Die Logon-App ist nicht ausschließlich auf Domänen-Benutzer festgelegt, sondern funktioniert auch mit lokalen Konten unter Windows sowie macOS, solange der lokale Benutzername jeweils mit dem Namen in AuthPoint übereinstimmt. Erwähnenswert ist die technische Einschränkung, dass die Logon-App nur in Kombination mit Benutzernamen und Passwörtern funktioniert, nicht aber mit biometrischen Anmeldefunktionen wie Touch-ID oder Windows Hello. Davon abgesehen hat uns AuthPoint durchweg begeistert, da es mit der lokalen und entfernten Anmeldung an Systemen einen Bereich absichert, der ohne Weiteres keine Unterstützung für MFA bietet.

Breite Unterstützung per SAML

Darüber hinaus integriert sich AuthPoint via SAML mit einer Vielzahl weiterer Anwendungen und Dienste. Die in der Online-Dokumentation enthaltene Liste der Integrationsanleitungen für Drittanbieter-Produkte würde den Umfang unseres Tests bei Weitem sprengen. Exemplarisch genannt seien Adobe, Amazon Web Services, Atlassian, Citrix, Google Workspace, Microsoft Office 365, VMware oder auch WordPress.

Viele dieser Anbieter statten ihre Lösungen zwar mit eigenen MFA-Verfahren aus, doch nutzen Endanwender mehrere davon, müssen sie sich mit den jeweiligen Eigenheiten der Drittanbieter vertraut machen. AuthPoint reduziert die Komplexität für Benutzer auf ein einheitliches MFA-Verfahren und zeigt Administratoren im Dashboard auf einen Blick, wie viele Authentifizierungen erfolgreich waren und wie oft Benutzer die Freigabe einer Anmeldung verweigert haben.

Absicherung von DNS-Abfragen

Zur Konfiguration von DNSWatchGO nutzten wir das separate Webfrontend, das gleichermaßen dem Schutz ganzer Netzbereiche mittels Firebox-Appliances wie auch einzelner Computer per Software-Client dient. Unter "Deploy / DNSWatchGO Clients" fanden wir den Download eines MSI-Pakets zur Installation unter Windows sowie einen Link zur Erweiterung für Google Chrome OS im Chrome Web Store. Für beide Varianten stellte uns die Webseite einen Account-API-Token bereit, sodass wir die Software unabhängig

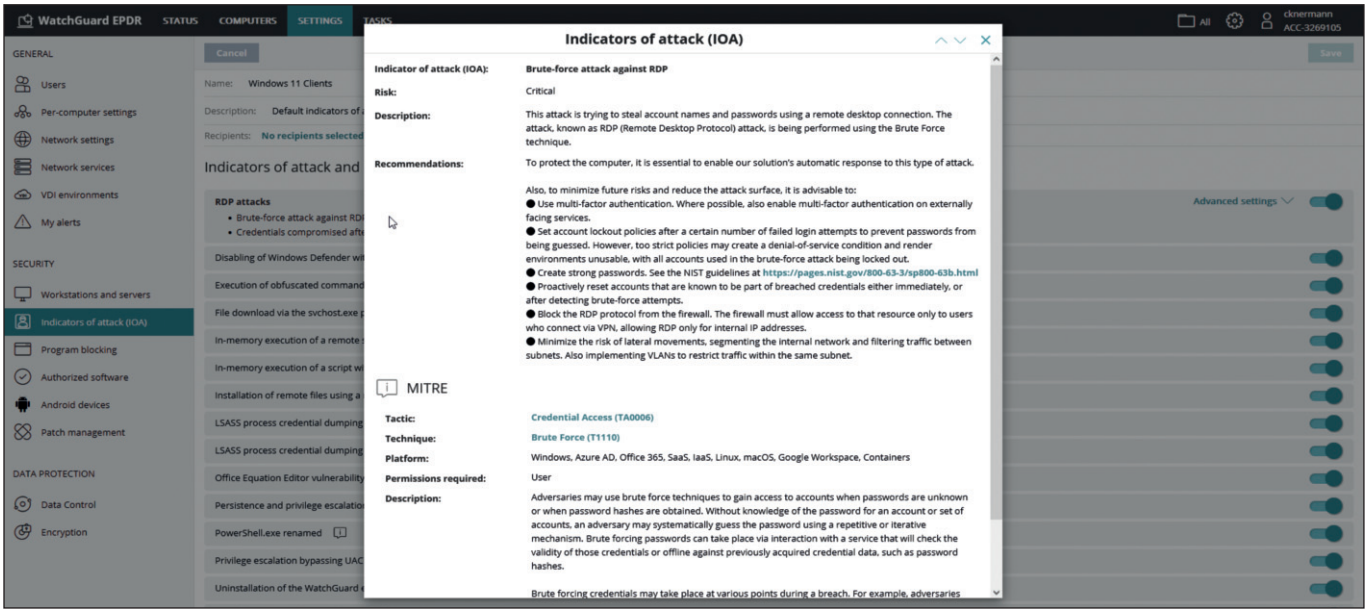

Bild 4: WatchGuard EPDR erkennt Hinweise auf fortgeschrittene Angriffstechniken.

von einer AD-Mitgliedschaft der Clients ausbringen konnten. Jeder Client, der sich mittels dieses Tokens in der WatchGuard-Cloud meldete, erschien automatisch im DNSWatchGO-Portal zugeordnet.

Im Fall von Chrome ließe sich die Erweiterung zwar auch in beliebige Instanzen des Chrome-Browsers integrieren. WatchGuard unterstützt jedoch offiziell nur den Einsatz unter Chrome OS und verpackte den Token in eine passende Konfigurationsrichtlinie, die wir direkt aus der Webseite in die Zwischenablage kopieren konnten. Per Google Admin Console zentral verwalteten Geräten mit Chrome OS Enterprise konnten wir dann die DNSWatchGO-Erweiterung mitsamt passender Konfiguration zuweisen.

Eingeschränkter Schutz durch DNS

Unter Windows ersetzt DNSWatchGO den bevorzugten DNS-Server des Systems durch die lokale Loopback-Adresse 127.0.0.1 und leitet sämtliche DNS-Anfragen durch den Softwareclient, der in der WatchCloud-Cloud nachfragt, ob es sich um eine zulässige Domain handelt oder nicht. In letzterem Fall leitet DNSWatchGO den Browser auf eine Hinweisseite um. Das funktioniert auch in Verbindung mit VPNs diverser Hersteller, allerdings bislang nur für klassische DNS-Anfragen und nicht für Browser, die DNS-over-HTTPS (DoH) verwenden.

Unter Chrome OS verankert sich DNSWatchGO als Erweiterung in den Webbrowser Chrome. Da dieser einen integralen Bestandteil des Betriebssystems bildet, sind Nutzer beim Surfen geschützt. Da aber in diesem Fall DNSWatchGO nicht den DNS-Server des Betriebssystems ändert, können Benutzer die DNSWatchGO-Richtlinien mithilfe von alternativen Browsern umgehen. Ein zuverlässiger Schutz lässt sich folglich nur gewährleisten, wenn Benutzer keine anderen Browser neben Chrome installieren dürfen.

Unerwünschte Domains filtern

Die passende Konfiguration von erlaubten und unerwünschten Webseiten konnten wir im Webfrontend festlegen. Dazu definierten wir zunächst unter "Configure / Content Filtering Policies" eine neue Richtlinie und durften aus einer umfangreichen Liste von über 40 zu blockierenden Themen wählen. Die Liste reicht von "Adult Material" mit mehreren Unterkategorien über "Drugs" und "Gambling" bis zu "Violence" und "Weapons".

Im Menü "Configure / DNSWatchGO Client Groups" erstellten wir dann eine Gruppe, in die wir unsere Clients einsortierten und ihnen so die Richtlinie zuwiesen. Auf den Clients konnten wir uns anschließend davon überzeugen, dass Domains aus einer der gesperrten Kategorien nicht mehr erreichbar waren und die Nutzer stattdessen auf eine Info-Seite umgeleitet wurden (Bild 2). Als Admin konnten wir im Webfrontend mittels "Configure / Search for a domain" herausfinden, aufgrund welcher Kategorie DNSWatchGO die jeweilige Domain blockierte. Im Fall erwünschter Domains konnten wir diese unter "Configure / Domain Allowlist" explizit wieder freigeben sowie umgekehrt gezielt einzelne Domains per Blocklist oder Filterlist zusätzlich sperren.

Worin besteht der Unterschied zwischen Blocklist und Filterlist? Eine Blocklist ist für gefährliche Seiten gedacht, von denen Malware- oder Phishing-Angriffe ausgehen. Domains, die wir als solche einstuften, konnten wir zur weiteren Analyse an WatchGuard übermitteln, sodass auch andere Kunden davon profitieren. Die Filterlist ist dagegen für Domains gedacht, die nicht unbedingt gefährlich, jedoch aus anderen Gründen im Unternehmen unerwünscht sind.

Über die Listen hinaus bedient sich DNSWatchGO diverser öffentlich erreichbarer Feeds, um als Quelle von Malware oder Phishing bekannte Domains zu blockieren. Auch Endanwender bemerken einen Unterschied: Gefilterte Domains leiten auf eine Seite um, die lediglich erklärt, dass die Domain nicht der Unternehmensrichtlinie entspricht. Im Falle gefährlicher Domains liefert eine alternative Seite zusätzliche Informationen, um über die Gefahren von Phishing aufzuklären.

Fortgeschrittene Malwareabwehr

Das dritte Modul WatchGuard EPDR konfigurierten wir über das separate Webfrontend, das sich uns ebenso intuitiv erschloss. So bot uns WatchGuard im Bereich "Computers" über die Schaltfläche "Add computers" die passenden Setuproutinen für Windows, macOS sowie Linux an. Wir konnten diese direkt herunterladen oder einen Link per E-Mail verschicken. Zur Installation der passenden App bot uns das Webfront einen QR-Code sowie die URL zur App im Google Play Store an.

Sobald wir einen ersten Client unter Windows installiert hatten, kümmerte dieser sich automatisch um eine "Discovery" und präsentierte uns eine Liste aller in seinem Netzwerksegment gefundenen Geräte mit der Option, auf kompatiblen Clients eine Remote-Installation anzustoßen. EPDR ist somit darauf ausgelegt, nicht nur in einer AD-Domäne befindliche Geräte, sondern auch alleinstehende Clients einzubinden.

Die Endpunkte verwalteten wir im Webfrontend wahlweise mittels dynamischer Filter oder in einer frei definierbaren Ordnerstruktur. WatchGuard hatte hier bereits diverse Filter nach Betriebssystemen, Typen von Systemen oder installierter Software vordefiniert, denen wir UND- sowie ODER-verknüpft beliebige weitere Abfragen hinzufügen konnten, um unsere Zielsysteme zu strukturieren. Um diese mit passenden Konfigurationen zu versorgen, legten wir in der Ordneransicht Unterverzeichnisse an, in die wir unsere Endpunkte einsortierten. Anschließend definierten wir unter "Settings / Security" Richtlinien für die verschiedenen Funktionsbereiche der EPDR, die wir dann den Ordnern mit unseren Endpunkten darin zuwiesen.

Die Funktionen von EPDR sind im Bereich "Security" des vertikalen Menüs zur Linken logisch strukturiert. Unter dem Punkt "Workstations and servers" konfigurierten wir die grundlegenden und fortgeschrittenen Mechanismen der Malware-Abwehr. Hierbei durften wir wählen, wie restriktiv die verhaltensbasierte Analyse ausführbarer Dateien vorgehen soll. Standard ist der Modus "Hardening", bei dem WatchGuard unbekannte Dateien aus dem Internet bis zu ihrer Analyse in der WatchGuard-Cloud blockiert, andere bereits lokale vorhandene Dateien aber zulässt (Bild 3). Exploit-Techniken blockiert EPDR in der Standardeinstellung komplett.

Auch für nicht per AD verwaltete Clients

Für Windows-Clients bringt WatchGuard eine eigene Software-Firewall mit, die die Windows-eigene Firewall ersetzt. Wie auch bei den übrigen Funktionen besteht der Vorteil vor allem für dezentrale Clients darin, dass diese Firewall komplett unabhängig von Domänenzugehörigkeit oder Gruppenrichtlinien und doch zentral konfigurierbar arbeitet. Ebenfalls nur auf Windows-Clients arbeitet die "Device Control", die extern angeschlossene Speichermedien und anderweitige Geräte zulässt oder sperrt.

Die "Web access control" orientiert sich an denselben Kategorien, die auch DNSWatchGO zum Sperren unerwünschter Webseiten nutzt. Im direkten Vergleich setzt DNSWatchGO aber noch früher an als EPDR, da DNSWatchGO bereits die DNS-Abfragen abfängt, bevor der Client versucht, eine Verbindung aufzubauen.

Im Bereich der "Indicators of attack (IOA)" listet WatchGuard zahlreiche Angriffstechniken auf, die EPDR erkennt. Dabei orientiert sich WatchGuard am online frei verfügbaren MITRE-ATT&ACK/D3FEND-Framework, erläutert mit Hilfetexten die Eigenheiten des jeweiligen Angriffsvektors und liefert Hintergrundinformationen zu den einzelnen Angriffstechniken mit direkten Links in die Datenbank von MITRE (Bild 4).

Das "Program Blocking" sperrt, ähnlich Microsofts AppLocker, Anwendungen anhand ihres Namens oder MD5-Hashes. Im Gegenzug konnten wir im Bereich "Authorized Software" bestimmte Anwendungen ausdrücklich freigeben. Der Bereich "Android devices" konfiguriert einen grundlegenden Schutz für mobile Geräte und kümmert sich neben Updates und Virenabwehr auch um einen Diebstahlschutz mit Erfassung des geografischen Standorts verlorener Geräte.

Die optionalen und separat zu lizenzierenden Zusatzmodule "Patch Management", "Data Control", eine inhaltsbasierte Analyse von Daten zum Schutz vor dem Abfließen schützenswerter Informationen, sowie "Encryption" sind nur für Windows-Betriebssysteme verfügbar – wiederum mit dem Vorteil, dass WatchGuard die Konfiguration unabhängig von AD oder Gruppenrichtlinien erledigt.

Fazit

WatchGuard hat mit Passport ein stimmiges Gesamtpaket geschnürt, das insbesondere Benutzern und Clients außerhalb eines gut gesicherten Netzwerks Schutz bietet. Dass sich die Administration der einzelnen Module noch auf drei separate Webinterfaces verteilt, ist zu verschmerzen, da sich die Bedienung jeweils ohne größere Einarbeitung intuitiv erschließt. Positiv überrascht hat uns der Funktionsumfang insbesondere von AuthPoint und der EPDR. Letztere punktet mit zentraler Verwaltung auch ohne Kontakt zu einem Active Directory. *(dr)* IT

So urteilt IT-Administrator

AuthPoint Logon App	8
AuthPoint-Drittanbieter-Integration	8
DNSWatchGO	6
EPDR-Funktionsumfang	7
EPDR-Clientunterstützung	8

Die Details unserer Testmethodik finden Sie unter www.it-administrator.de/testmethodik

Dieses Produkt eignet sich

optimal für Unternehmen mit vielen mobilen Benutzern und Clients auch ohne AD-Anbindung.

bedingt für Unternehmen, die bereits Teile der Funktionalität mit anderweitigen Tools gelöst haben.

nicht für Unternehmen mit homogener Infrastruktur, die bereits umfassende Sicherheitsmaßnahmen implementiert haben.