WatchGuard Threat Detection & Response

Zur Gefahrenlage für KMU

Berichte über Cyberangriffe gegen Großkonzerne machen Schlagzeilen. Was die Öffentlichkeit jedoch nicht erfährt: Auch KMU und dezentral aufgestellte Unternehmen fallen diesen Malware-Angriffen zum Opfer. Tag für Tag. Der U.S. Securities and Exchange Commission zufolge sind KMU sogar das Hauptziel für Internetkriminalität. Im Jahr 2014 richteten sich über 60 % aller gezielten Cyberangriffe gegen KMU. 75 % der Spear-Phishing-Versuche nehmen KMU ins Visier.

Für KMU fallen die Kosten, die mit diesen Angriffen einhergehen, besonders ins Gewicht. Viele dieser Unternehmen, genauer gesagt ungefähr die Hälfte, stellen in den ersten sechs Monaten nach einem Cyberangriff den Betrieb ein. KMUs müssen sich den gleichen Gefahren stellen wie Großkonzerne, nur mit deutlich knapperen Budgets und weniger Ressourcen. Wie können KMU den Kampf gegen Cybercrime gewinnen, ohne in den Ruin zu steuern?

Im Jahr **2014** richteten sich über **60 %** aller **gezielten Cyberangriffe** gegen **KMU**, **75 %** des **Spear-Phishing** nimmt **KMU** ins Visier.

Signaturen sind kein Universalmittel

Hacker wissen genau, wie Sicherheitsanbieter ticken. Die Kriminellen sind längst auf eine neue Form von Malware ausgewichen. Eine, der Antivirenprogramme nichts anhaben können. Diese Malware infiziert zunächst ein paar Unternehmen, bevor sie enttarnt wird. Die Sicherheitsunternehmen erstellen dann rasch eine Signatur, um zukünftige Angriffe abzuwehren. Wenn die Malware einige Male gesperrt wurde, stampfen sie die Verbrecher entweder komplett ein oder lassen einen Obfuscator darüber laufen, um die Signatur zu ändern. Der Vorgang wiederholt sich bei neuen Malware-Varianten und neuen Signaturen stets von Neuem.

Seit einigen Jahren ist jedoch eine Tendenz weg von Signaturen als Universalmittel zu erkennen. Die Sicherheitsanbieter werden immer besser und gehen mit einem anderen Ansatz an die Malware heran – durch Erkennen und Unterbinden von Verhalten, das Malware-Bedrohungen brauchen, um erfolgreich zu sein. Die Varianten sind nicht in allen Aspekten gleich oder laufen nach demselben Schema ab, haben aber im Groben ähnliche Verhaltensmuster, die zur Verbesserung der Erkennungsrate ermittelt werden können.

Malware-Verhaltensmuster

Malware ist kein großes Geheimnis. Hacker ändern zwar ständig ihre Taktiken und Angriffsmethoden, aber ein paar Verhaltensweisen sind den meisten Malware-Varianten gemein.

Hier ein paar gängige Ansätze:

- In ein Microsoft-Makro wird ein Link zu einem Malware-Host eingefügt, wodurch die Malware heruntergeladen und ausgeführt wird
- Reproduziert und löscht sich selbst, um Erkennungstechnologien zu umgehen
- Versuch, durch Manipulation der Mechanismen zur Steuerung des Benutzerzugriffs und der Berechtigungen im Kernel des Betriebssystems Administratorrechte zu erlangen
- Modifizierung von Dateien oder Prozessen durch Injektion bösartiger Komponenten
- Löschen originaler Systemdateien und Ersetzen dieser durch bösartige Kopien mit demselben Dateityp und demselben Namen

Signaturen sind zwar schön und gut, wenn es um die Abwehr bekannter Bedrohungen geht, aber Unternehmen brauchen darüber hinaus auch wirksame Maßnahmen zum Stoppen unbekannter oder neuer Malware-Varianten. Eine Nachverfolgung von Verhaltensmustern wie oben ermöglicht die Erkennung neuer Malware-Varianten, unabhängig von Änderungen, die an der Signatur vorgenommen werden.

Erkennung mit TDR

Threat Detection and Response, der neue Sicherheits-Service von WatchGuard, vereint durch den WatchGuard Host Sensor mehrere Erkennungsformen zum Aufspüren selbst raffiniertester Malware-Bedrohungen.

Signaturen – Wie bereits erwähnt sind Signaturen ein wichtiges Instrument zur Verteidigung gegen Malware. Die Liste der bekannten Bedrohungen muss stets aktuell sein. WatchGuard Threat Detection and Response nutzt Bedrohungsanalysen auf Enterprise-Niveau zur Beurteilung, ob es sich bei einem verdächtigen Ereignis um eine bekannte Bedrohung handelt.

Heuristik – Statt sich auf Signaturen zu verlassen, sucht TDR anhand von Regeln oder Algorithmen nach Befehlen, die auf bösartige Absichten hindeuten könnten. Diese Erkennungsmethode kann eine Bedrohung im Nu erkennen, ohne dass diese ausgeführt wurde. TDR setzt mit dem WatchGuard Host Sensor über 175 Heuristiken ein.

Verhaltensanalyse – Da Malware-Bedrohungen bestimmten Verhaltensmustern folgen, trägt die Verfolgung dieser Schritte zuverlässig zur Erkennung unbemerkter Malware-Varianten bei. Das Host Ransomware Prevention-Modul beobachtet Verhaltensmuster, die traditionell mit Ransomware-Angriffen in Zusammenhang stehen, um diese Angriffe gezielt zu verhindern, bevor die Dateien verschlüsselt werden.

Netzwerkerkennung – Das Netzwerk ist eine wichtige Informationsquelle in Bezug auf Angriffe und Leistungsnutzung. Wer Einblick in Muster zu ungewöhnlichen oder gesperrten Datenbewegungen und Besuchen bösartiger oder bedrohter Websites gewinnt und Botnets und andere Bedrohungen zu erkennen vermag, hat schon viel für den Schutz des Unternehmens erreicht. Unter Zuhilfenahme der branchenführenden Lösungen für erweiterte Network Security erfasst und erkennt TDR Bedrohungen für das Netzwerk.

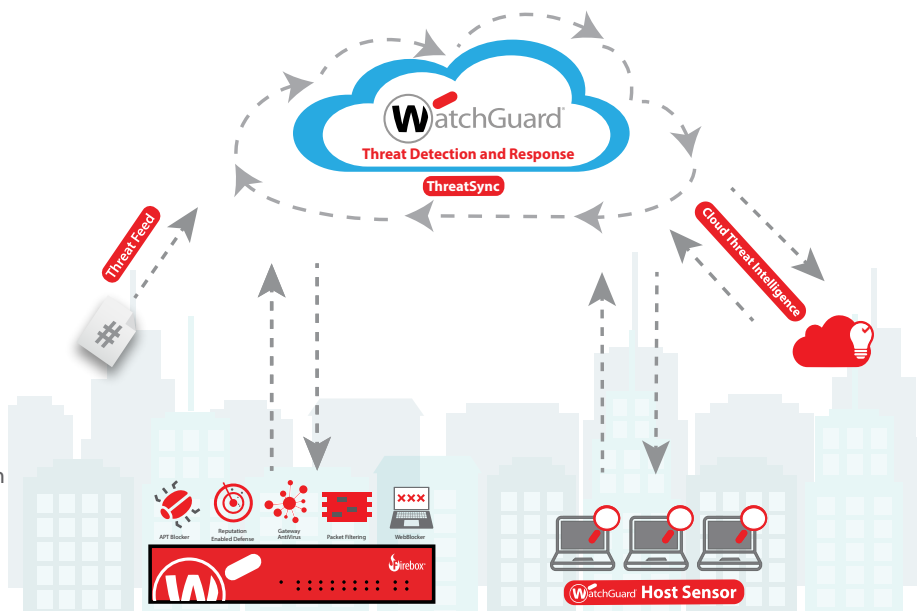
Was Korrelation leistet

Die Erfassung von Daten aus verschiedenen Quellen ist in puncto Sicherheit schon recht clever. Stehen diese Quellen jedoch für sich allein, ist der Überblick über Ihr Unternehmen unzureichend. Korrelation fügt die einzelnen Informationen aller Sicherheitsdienste zusammen, damit diese gemeinsam Sinn ergeben. Indem Sie Daten aus mehreren Quellen zueinander in Bezug setzen, verkürzen Sie die zur Erkennung und Abwehr von Bedrohungen erforderliche Zeit. Die IT-Administratoren können klar erkennen, welche Bedrohungen am gravierendsten sind und sofortiges Handeln erfordern.

Vollständiger Überblick mit ThreatSync

Korrelation ist die einzige Möglichkeit, einen vollständigen Überblick über die Sicherheit in Ihrem Unternehmen zu erhalten. ThreatSync ist die neue Cloud-basierte Engine von WatchGuard zur Korrelation und Bewertung von Bedrohungen. Sie liefert verwertbare Einblicke zu Angriffen auf das Netzwerk und die Endpunkte.

ThreatSync erfasst selbst Ereignisdaten von der WatchGuard Firebox und dem WatchGuard Host Sensor, setzt diese mit aktuellen Cloud-basierten Informationen zur Bedrohungslage in Verbindung und analysiert sie. Über spezifische Algorithmen ergibt sich ein solides Fundament für die Bewertung von Gefahren und das Ergreifen entsprechender Abwehrmaßnahmen. Hierfür gruppiert ThreatSync ähnliche Bedrohungen und hebt Vorfälle, auf die reagiert werden sollte, hervor.



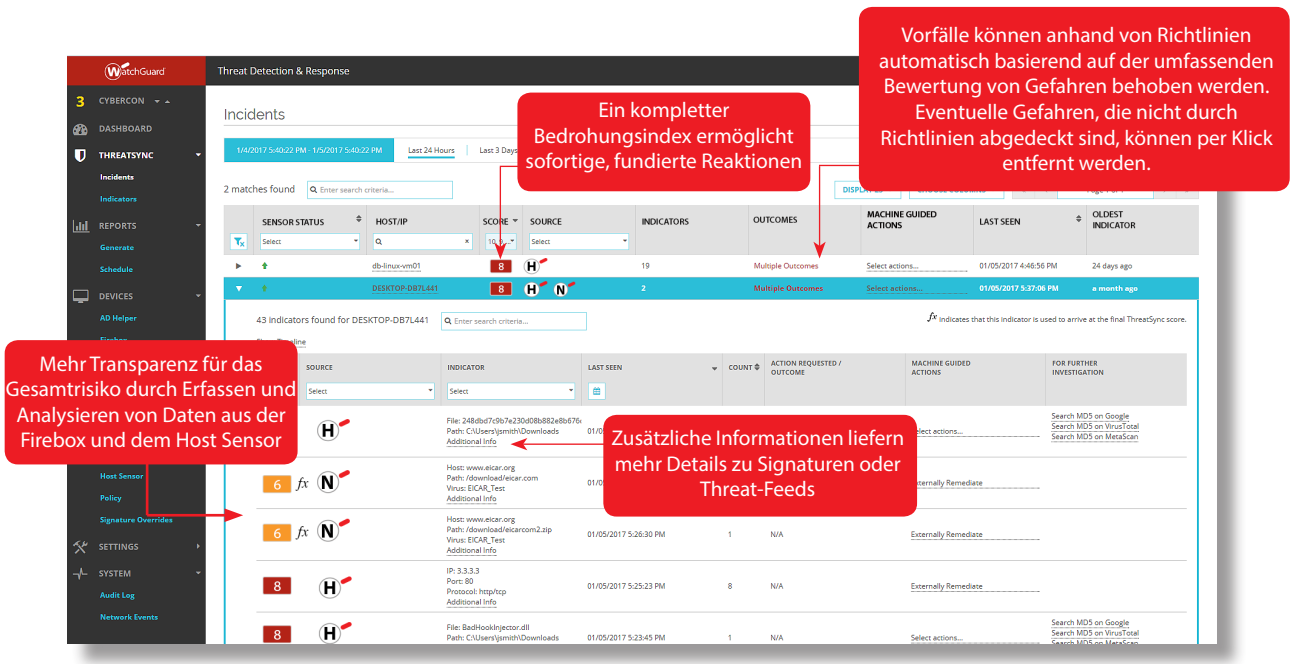
Somit liefert ThreatSync nicht nur umfassende Einblicke in die Vorgänge, die im Netzwerk und am Endpunkt ablaufen. Durch die gezielte Bewertung können die Sicherheitsverantwortlichen auch im Handumdrehen erkennen, welche Bedrohungen am gefährlichsten sind und umgehende Aufmerksamkeit erfordern. Auf Basis der Priorisierung der Gefahren lassen sich Angriffe deutlich schneller identifizieren und geeignete Abwehrmaßnahmen ergreifen. Darüber hinaus lässt sich die Anzahl der dedizierten Ressourcen verringern, die zum Entfernen von Bedrohungen erforderlich sind.

Das Beste: Sie können ThreatSync jetzt konfigurieren, um automatische E-Mail-Benachrichtigungen zu erhalten, wenn Zwischenfälle und Indikatoren entdeckt und Bedrohungen abgewehrt werden. Diese Warnungen enthalten genaue Informationen zu Bedrohungen des Netzwerks und des Endpunkts – ohne vorherige Anmeldung im Dashboard. So können Sie die Sicherheit stets im Auge behalten – egal, wo Sie sind.

Automatisierte Reaktionen mit TDR

Für KMU mit begrenzten Mitteln oder dezentral aufgestellte Unternehmen ohne entsprechend geschulte Techniker an den einzelnen Standorten ist es mitunter problematisch, auf jede Bedrohung angemessen zu reagieren. Automatisierung kann hier für die schnelle und effektive Erkennung und Abwehr von Bedrohungen den Ausschlag geben. Durch automatisierte Reaktionen können Unternehmen ihre knappen Ressourcen anderen Sicherheitsbelangen widmen. Darüber hinaus wird die Zeit zur Behebung verbessert, wodurch sich die Infektionszeit verkürzen lässt, damit der normale Betrieb schnellstmöglich wieder aufgenommen werden kann.

Mit WatchGuard TDR können Benutzer schnell und unkompliziert Richtlinien erstellen, um die Automatisierung auf Grundlage der betrieblichen Anforderungen umzusetzen. ThreatSync ermöglicht die Bewertung und Priorisierung von Bedrohungen. So können Benutzer Richtlinien zur Behebung anhand eines Bedrohungsindex oder -bereichs einrichten. Die Maßnahmen reichen von der Isolierung der Datei über das Löschen des Registrierungsschlüssels bis hin zum Abbruch des Prozesses. So kann beispielsweise bei einer niedrigen Bedrohungslage die Automatisierung von Reaktionen erst für einen Bedrohungsindex ab 8 festgelegt werden. Sollte sich jedoch eine massivere Bedrohungslage einstellen, kann die automatische



Über WatchGuard

WatchGuard Technologies gehört zu den führenden Anbietern im Bereich Netzwerksicherheit. Mehr als 75.000 Unternehmen weltweit vertrauen auf die ausgeklügelten Schutzmechanismen auf Enterprise-Niveau, wobei dank der einfachen Handhabung insbesondere kleine bis mittlere sowie dezentral aufgestellte Unternehmen vom Einsatz profitieren. Neben der Zentrale in Seattle im US-Bundesstaat Washington verfügt WatchGuard über Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. Weitere Informationen finden Sie unter WatchGuard.de.

Wenn Sie mehr über WatchGuard, unsere Werbeaktionen und Updates erfahren möchten, folgen Sie uns auf Twitter @WatchGuard, auf Facebook oder LinkedIn. Lesen Sie auch unseren InfoSec-Blog Secplicity. Darin wird einfach und nachvollziehbar beschrieben, wie Sie den neuesten Bedrohungen am besten begegnen. Hier geht's zum Blog: www.secplicity.org

Deutschland, Österreich, Schweiz: +49 700 92229333 INTERNATIONALER VERTRIEB +1.206.613.0895 www.watchguard.de