INTRUSION DETECTION FÜR KMU

Wenn die Firewall versagt

Paul Becker
Technical Content

Cyberattacken können heute jedes Unternehmen treffen. Dabei können die Ziele der Angreifer vielseitig sein. Sie können die Absicht verfolgen, Ransomware auf dem System zu installieren, um die IT-Landschaft zu verschlüsseln und eine Lösegeldforderung zu stellen. Hacker können es darauf abgesehen haben, ein Botnetz aufzubauen, sodass die IT des Opfers für zukünftige Cyberattacken, wie etwa DDoS-Angriffe, genutzt werden kann. Oder aber der Eindringling hat es auf den Diebstahl von Daten abgesehen. Zum Beispiel von Kundendaten, um sie im Anschluss im Darknet zu verkaufen. Gezielte Attacken können es auch auf das Know-How des Unternehmens abgesehen haben, um Industrie- oder Wirtschaftsspionage zu betreiben.

Auch kleine und mittlere Unternehmen müssen sich angesichts der vielschichtigen Bedrohung daher gegen Cyberattacken rüsten. Häufig fallen Angriffe auf die IT-Landschaft lange Zeit nicht auf. Durchschnittlich dauert es 200 Tage, bis sie bemerkt werden. In dieser Zeit können sie großen Schaden anrichten. Damit Angriffe unmittelbar erkannt werden, hilft ein Intrusion Detection System (IDS), auf das auch KMU setzen sollten.

Was ist ein Intrusion Detection System (IDS)?

Ein Intrusion Detection System ermöglicht, Attacken, die auf das Netzwerk, einzelne Server oder Clients ausgeführt werden, zu erkennen.

Je nach System unterscheiden sich die Funktionsweisen von Intrusion Detection Systemen, sowohl was die Implementierung als auch die Verfahren zur Einbruchserkennung angeht. IDS können sowohl auf Signaturen und Filter zugreifen, die spezifische Angriffsmuster beschreiben, aber auch heuristische Methoden verwenden, die Abweichungen von einem Normalzustand erkennen.

Dazu analysieren IDS zum einen die Netzwerkpakete, beispielsweise mit einer Deep Packet Inspection (DPI). Im Gegensatz zu einer Firewall schaut eine IDS auch auf den Inhalt der Netzwerkpakete, anstatt nur Absender und Empfänger auf Rechtmäßigkeit zu überprüfen. Sie ist daher eine wichtige Ergänzung zur Firewall. Zum anderen ziehen viele Systeme auch weitere Daten in ihre Analyse ein, die sie direkt von Servern und Clients beziehen.

Netzwerkbasiert (NIDS) oder hostbasiert (HIDS)

Welche Daten dem IDS zu Verfügung stehen, hängt im Wesentlichen davon ab, wo der oder die Sensoren im Netzwerk platziert sind. Dabei lässt sich eine grundsätzliche Unterscheidung treffen: Entweder findet die Analyse netzwerkbasiert (NIDS) oder hostbasiert (HIDS) statt. Bei einer netzwerkbasierten Analyse wird der Sensor entweder durch eine Appliance an einen Switch mit Mirror-Port realisiert oder durch eine Komponente im Netzwerk, durch die jeglicher Netzwerkverkehr durchfließen muss. Das kann zum Beispiel ein Unified Threat Management (UTM) oder eine Next Generation Firewall (NGFW) sein. Bei einer hostbasierten Überwachung wird der Sensor direkt auf den Hosts (zum Beispiel Server, Client, IoT-Gerät) platziert, indem ein entsprechender Dienst installiert wird.

IDS für KMU

Ein Intrusion Detection System ist nicht nur für Großunternehmen interessant, sondern auch für kleine und mittlere Unternehmen von großer Bedeutung. Während Großunternehmen mit einer mannstarken IT-Abteilung für Administration und Forensik, Speziallösungen einsetzen können, die NIDS und HIDS in komplexen hybriden Ansätzen kombinieren, fehlen KMUs dafür die fachlichen sowie finanziellen Mittel.

Die Anforderungen von KMUs an eine IDS lauten:

- Sie brauchen statt einem Spezialtool eine integrierte Lösung, die im Administrations-Alltag vielseitig eingesetzt werden kann und mehrere Fliegen mit einer Klappe schlägt.
- Weder der administrative noch der finanzielle Aufwand, die Lösung einzuführen, darf zu groß sein. Hohe, einmalige Rüstkosten sind für KMU nicht zu stemmen.
- Die laufenden Kosten dürfen nicht zu hoch sein.
- Die Bedienung muss verständlich sein, damit die Mitarbeiter das Tool effektiv einsetzen können und gerne benutzen.

Die zentrale Variante: eine UTM oder NGFW

Beliebt und seit vielen Jahren bei KMU im Einsatz sind Unified Threat Management-Systeme (UTM). Sie bündeln viele Sicherheits-Features in einer einzelnen Appliance und Software-Oberfläche. Häufig wird die Software dabei direkt auf der Hardware mit ausgeliefert. Das fertige System muss dann nur noch angeschlossen und konfiguriert werden.

Platziert wird die UTM in der Regel zwischen Internet und lokalem Netzwerk. Jeglicher Traffic, der das lokale Netzwerk in Richtung Internet verlässt, durchläuft dadurch ebenso die UTM wie alle Netzwerkpakete, die vom Internet in das lokale Netzwerk eintreten. Die UTM wird so zur zentral platzierten Überwachungseinheit im Unternehmen. Alternativ lassen sich auch mehrere UTM-Systeme zwischen Netzwerksegmenten platzieren. Die UTM führt also eine netzwerkbasierte IDS durch. Darüber hinaus unterscheidet sich der Funktionsumfang je nach Anbieter und Version. Neben einem Intrusion Detection System (IDS) umfasst er meist eine klassische Firewall, VPN und Proxy-Funktionen, Sandboxing für E-Mails, Content-Filter oder auch die Möglichkeit regelmäßiger Penetrationstests.

Next Generation Firewalls (NGFW) wurden ursprünglich als Ergänzung zu einer UTM entwickelt, um Performance-Probleme von UTMs zu beheben. Sie lieferten höhere Durchsatzraten, waren weniger auf die einfache Bedienung und den großen Funktionsumfang ausgelegt. Mittlerweile haben sich die beiden Lösungen jedoch immer weiter angenähert. Die Performance-Probleme von UTM-Systemen wurden durch die technische Entwicklung verkleinert und der Funktionsumfang von NGFW-Lösungen ausgebaut. Manche Anbieter vermarkten ihre Lösungen inzwischen auch als „UTM Next Generation Firewall“. Die Begriffe NGFW und UTM lassen sich daher oft synonym verwenden.

Vor- und Nachteile einer UTM/NGFW

Attraktiv machen UTM/NGFW-Systeme die relativ günstigen Rüstkosten. Die Lizenzkosten für viele Einzeltools entfallen und die Preisgestaltung vieler Anbieter ist auch für kleine und mittlere Unternehmen realistisch. Bei Administratoren sind sie zudem beliebt, weil sie nur noch ein einzelnes System zu betreuen haben, was Übersicht schafft und Zeit spart. Insbesondere da viele Anbieter die Benutzeroberfläche übersichtlich halten und die Bedienung daher leichtfällt.

Wie bereits ausgeführt, muss der gesamte Netzwerktraffic, der das lokale Netzwerk oder Segmente verlässt, durch die UTM oder NGFW geroutet werden. Damit stellen die Systeme aus dem Blickwinkel der Performance einen limitierenden Faktor dar. Es besteht bei hoher Auslastung oder gewachsener IT-Umgebung die Gefahr, dass die Systeme zu einem Flaschenhals werden. Die Performance ist schließlich auf die Ressourcen der einzelnen Appliance beschränkt. Eine Skalierbarkeit ist zwar gegeben, aber aufwendig, da die Hardware nachgerüstet werden muss.

Auch Geräte, die sich nicht im Firmennetzwerk befinden, ziehen Probleme nach sich. Damit eine UTM ein im Homeoffice eingesetztes Notebook überwachen kann, muss sämtlicher Traffic mit einem VPN durch das Firmennetzwerk geroutet werden. Das ist nicht nur teuer, sondern sorgt auch für einen Einbruch in der Performance. Auch außerhalb des Firmennetzwerks befindliche Server lassen sich nicht ohne weiteres in ein gemeinsames Überwachungssystem integrieren. Die genannten Faktoren betreffen alle Funktionen der UTM, von der das Intrusion Detection System nur einen Teil darstellt. Wie sieht es im speziellen mit den IDS-Funktionen aus? Die netzwerkbasierte IDS von UTM oder NGFW-Systemen hat ihre Stärke darin, Angriffe von außen zu erkennen. Wird über das Internet gezielt die IT-Umgebung des Unternehmens ausspioniert oder angegriffen, können sie einen Alarm schalten. Haben die Angriffe jedoch die erste Verteidigungslinie überwunden oder sind nicht durch das Internet durchgeführt worden, lassen sie sich nicht aufspüren oder gar nachverfolgen.

»Haben die Angriffe jedoch die erste Verteidigungslinie überwunden, lassen sie sich nicht aufspüren oder gar nachverfolgen.«

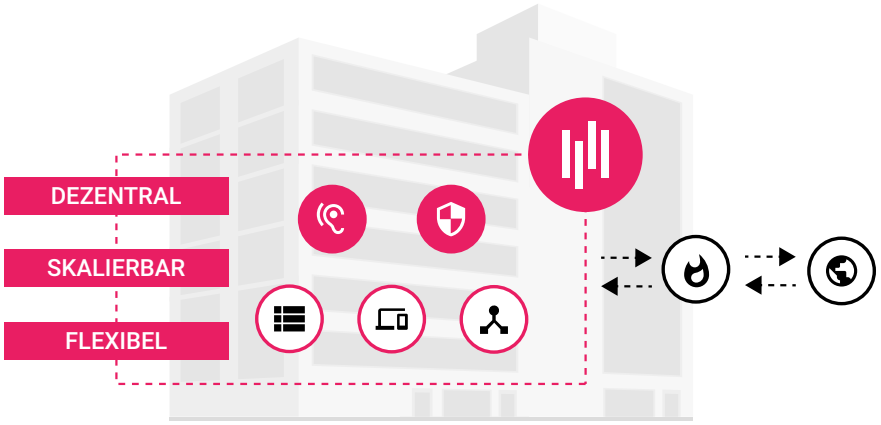
Als zentrale Einheit der IT-Infrastruktur bieten UTM-Systeme die Möglichkeit Sicherheitsstrategien und Konzepte schnell umzusetzen, ohne die gesamte IT-Landschaft umkrempeln zu müssen. Die Appliance wird entsprechend im Netzwerk platziert, Konfigurationen vorgenommen und es kann los gehen. Eben dieser zentrale Charakter kann jedoch auch negative Folgen haben. Die UTM stellt nämlich einen Single Point of Failure dar. Werden zu Beginn oder im Betrieb falsche Konfigurationen vorgenommen, ist die Sicherheit der gesamten Infrastruktur gefährdet. Auch fehlende Updates des Systems können schwerwiegende Sicherheitsfolgen haben. Eine weitere Gefahr stellt dar, dass die UTM-Appliance einmal ganz ausfallen könnte. In diesem Fall steht der Administrator vor zwei Möglichkeiten: Auf die Sicherheitsmechanismen verzichten oder die IT des Unternehmens komplett herunterfahren und damit die Arbeit im Unternehmen lahmlegen.

Die dezentrale Variante: IDS mit Enginsight

Einen in der Implementierung gegensätzlichen, dezentralen Ansatz bietet die Software Enginsight. Ebenso wie eine UTM handelt es sich um eine integrierte IDS. Die Intrusion Detection stellt nur eine Komponente eines umfangreichen Featuresets dar.
Der Funktionsumfang von Enginsight umfasst unter anderem die Überwachung von Server und Clients von innen mittels Agent, eine Asset Discovery aller Geräte mit IP-Adresse sowie das automatisierte pentesten ebendieser. Darüber hinaus lassen sich Webanwendung auf Verfügbarkeit und Sicherheit überwachen. Das IDS ist Teil der Überwachung von Server und Clients via Agent und damit hostbasiert. Auch wenn sich die Funktionen teilweise mit UTM oder NGFW-Firewall-Systemen überschneiden, liegt der Fokus bei Enginsight mehr auf der Hygiene der gesamten IT-Landschaft als auf einer möglichst starken ersten Verteidigungslinie.

Wie funktioniert das IDS von Enginsight?

Grundlage der Intrusion Detection ist bei Enginsight eine Analyse der Netzwerkpakete direkt auf dem Host mittels Deep Packet Inspection (DPI). Das heißt, Enginsight prüft nicht nur, woher die Netzwerkpakete kommen, sondern unterzieht auch den Inhalt der Netzwerkpakete einer Prüfung. Die DPI erkennt so Cyberattacken, ganz unabhängig von wo sie kommen. Sowohl Angriffe über das Internet als auch solche, die sich bereits im internen Netz ausbreiten.
Der hostbasierte Ansatz ermöglicht, weitere Analysedaten neben der DPI in die Intrusion Detection einzubeziehen und miteinander zu kombinieren. Dazu bieten sich beispielsweise die klassischen Monitoring-Daten an, wie die Auslastung von CPU, RAM oder



Netzwerkkarte. Die Machine-Learning-Komponente von Enginsight analysiert die Metriken des Monitorings auf Anomalien. Treten gleichzeitig verdächtige Netzwerkaktivitäten und Anomalien der CPU auf, spricht dies für eine erfolgreiche Cyberattacke. Auch das gleichzeitige Öffnen eines neuen Ports kann ein solches Anzeichen sein. Weitere Ansatzpunkte für die Erkennung eines erfolgreichen Eindringens liefert der Mitschnitt sicherheitsrelevanter Systemevent, zum Beispiel von erfolgreichen und nichterfolgreichen Login-Versuchen. Die Intrusion Detection von Enginsight ist unabhängig davon, wo sich die überwachten Geräte befinden. Verlassen Notebooks das Firmennetzwerk, etwa weil ein Mitarbeiter ins Home-Office wechselt, bleibt das IDS aktiv, ohne dass der Traffic via durch das Firmennetzwerk geroutet werden muss. Das erhöht die Flexibilität enorm und verhindert Performance-Probleme. Auch in ein externes Rechenzentrum ausgelagerte Server lassen sich einfach in das IDS integrieren.

Durch die Analyse auf dem Host kann auf eine extra Hardware bei der Nutzung von Enginsight als SaaS komplett zu verzichten. Weder ein Applikationsserver oder besonderer Switch müssen vorhanden sein. Es muss lediglich der Pulsar Agent auf dem Server oder Client installiert werden, die Analyse der Netzwerkdaten aktiviert und die Überwachung startet ganz ohne weiteren Konfigurationsaufwand. Somit bietet Enginsight eine noch einfachere Implementierung als eine UTM. Die nicht vorhandenen Rüstkosten für Hardware, wenigen Arbeitsstunden beim Start und das flexible Preismodell machen Enginsight auch aus finanzieller Sicht attraktiv. Erst recht, weil sich dank des umfassenden Funktionsumfangs andere Tools abschaffen und deren Lizenzkosten einsparen lassen.
Soll zusätzlich zur hostbasierten eine netzwerkbasierte Intrusion Detection vorhanden sein, lässt sich der Enginsight Pulsar Agent auch auf einer Linux- oder Windows-Appliance installieren, die an den Mirror Port eines Switches angeschlossen wird. Mit einem geringen Mehraufwand erlaubt Enginsight so, ein hybrides System zu etablieren. Diese Möglichkeit macht das IDS von Enginsight auch für große Mittelständler oder Großunternehmen interessant.

Beispiele: Zwei Angriffsszenarien

Eine Cyberattacke verläuft meist nach dem folgenden Schema: Der Angreifer versucht sich an einem Punkt in der IT-Infrastruktur des Opfers einzunisten, um sich von dort aus weiter auszubreiten. Der erste Angriffspunkt muss daher nicht gleich das Ziel einer Attacke sein, sondern kann auch ein weniger interessantes System sein. Anstatt also gleich den Server mit den bedeutenden Firmeninternas, wird erst der PC eines Mitarbeiters attackiert, der gar nicht unbedingt unmittelbar Zugriff auf die Zieldaten besitzen

muss. Das Anliegen ist es zunächst, überhaupt in das lokale Netzwerk zu gelangen, die erste Verteidigungslinie zu überwinden.

Angriff via E-Mail

Weiterhin das meistgenutzte Einfallstor für verschiedene Arten von Cyberangriffen bleibt die E-Mail. Dazu sendet der Angreifer eine E-Mail mit infiziertem Anhang oder Link zu einer infizierten Webseite an einen oder mehrere Mitarbeiter eines Unternehmens. Er setzt darauf, dass der Mitarbeiter den Anhang öffnet oder auf den entsprechenden Link klickt.
Im besten Fall erkennt ein Analysesystem den schädlichen Inhalt der E-Mail und verhindert, dass sie überhaupt zugestellt wird. Viele UTMs liefern dafür eine E-Mail-Sandboxing-Funktionalität. Dort werden E-Mail in einer abgeschotteten Umgebung geöffnet und deren Verhalten im virtuellen System geprüft. Die Entwickler von Malware haben allerdings auf den Einsatz von Sandboxes reagiert. Viele schädliche Programme erkennen, wenn es sich um eine Überprüfung in einem Test-System handelt und legen dann ein harmloses Verhalten an den Tag.
Das heißt: Auch wenn eine Sandbox zum Einsatz kommt, kann es vorkommen, dass Malware diese Hürde überwindet. In der Folge hat es der Eindringling in das lokale Netzwerk geschafft und kann sich an die Arbeit machen. Vom PC des Mitarbeiters, der die E-Mail geöffnet hat, beginnt er, sich im Netzwerk umzuschauen. Zudem baut er von innen nach außen eine Verbindung mit einem System des Angreifers auf, um Informationen mitzuteilen oder neue Anweisungen zu erhalten.

Die zentral implementierte UTM steht nun vor einem Problem: Erstens kann sie das unrechtmäßige Verhalten im Netzwerk nicht erkennen, da sie ihren Sensor ausschließlich an der Schwelle zwischen Internet und lokalem Netz sitzen hat. Zweitens hat sie auch Schwierigkeiten die unrechtmäßige Verbindung der Malware mit dem System des Angreifers zu erkennen, da der Verbindungsaufbau von Seite des vermeintlich vertrauenswürdigen PCs stattfindet.

Die dezentrale, hostbasierte Intrusion Detection von Enginsight jedoch kann auch innerhalb des lokalen Netzwerkes für Cyberattacken typisches Verhalten aufspüren. Startet ein PC eines Mitarbeiters einen umfangreichen Port-Scan, um das Netzwerk auszuspionieren oder Bruteforce-Attacken, um sich auf Servern einzuloggen, erkennt dies die Deep Packet Inspection und gibt eine entsprechende Warnung aus.

Angriff via USB-Stick

Der Versand von Malware via E-Mail ist die häufigste Methode, mit der Angreifer versuchen im lokalen Netz Fuß zu fassen. Eine andere Möglichkeit sind externe Speichermedien, die Mitarbeiter in das Unternehmen einführen oder von einer dritten Person eingeführt werden. Das kann ein vermeintlich verlorener USB-Stick auf dem Parkplatz sein, den ein Mitarbeiter aus Neugier mit seinem PC verbindet. Oder aber einem Angreifer gelingt, physisch in die Büroräume einzudringen und verbindet ein Speichermedium selbst mit einem PC oder Server. Um einen solchen Fall zu verhindern, sind verschlossene Bürotüren und die Schulung von Mitarbeitern zentral. Gänzlich ausschließen, dass es dennoch zu einem solchen Vorfall kommt, kann man jedoch nicht. In dem Speichermedium-Szenario sind zentrale Systeme, wie normale Firewalls, NGFW oder UTM-Systeme gänzlich machtlos, da sie nur den technischen Weg in das lokale Netz via Internet absichern. Dezentrale Lösungen wie Enginsight, sind hier im Vorteil. Die Aktivitäten der Schadsoftware werden wie beschrieben erkannt.

Fazit

Ein Intrusion Detection System stellt eine sinnvolle Ergänzung zu einer einfachen Firewall und Anti-Viren-Software dar. Die Implementierung, der Betrieb und die Bedienung kann dabei einfach realisiert werden, sodass auch kleine und mittlere Unternehmen problemlos einsetzen können. Unified Threat Management-Systeme ebenso wie Enginsight bieten IDS-Lösungen, die in ein größeres Feature-Set integriert werden. Das spart Zeit, Nerven und Lizenzkosten im Vergleich zum Einsatz von mehreren Einzeltools. Während UTM oder NGFW-Systeme jedoch ausschließlich eine netzwerkbasierte Intrusion Detection an bestimmten Punkten im Netzwerk (zwischen Segmenten oder zwischen Internet und lokalem Netz) bieten, lässt sich die IDS von Enginsight flexibler und dezentral implementieren. So werden auch Cyberattacken, die sich bereits im lokalen Netzwerk befinden, erkannt. Darüber hinaus ermöglicht die hostbasierte Umsetzung, mehr Daten in die Analyse zu integrieren.

Jenseits des Intrusion Detection Systems unterscheiden sich jedoch der Funktionsumfang von UTMs und Enginsight deutlich. Daher ist UTM und Enginsight nicht unbedingt eine Wenn-Oder-Entscheidung. In Mittleren Unternehmen können sie sich im Gegenteil gut ergänzen. Gerade in kleineren Unternehmen, die Enginsight einsetzen, reicht jedoch zur Ergänzung oft auch eine einfache Firewall im Router.