Der nächste Schritt für Next-Gen-Virenschutz

Cyberangriffe sind auf dem Vormarsch und eine wachsende Anzahl von Endpunkten bietet Gegnern immer mehr Möglichkeiten, auf die vertraulichen Daten Ihres Unternehmens zuzugreifen. Zu viele Unternehmen verlassen sich beim Schutz dieser Endpunkte immer noch auf signaturbasierte, veraltete Antivirentools. Leider können alte Antivirenprogramme – sogar wenn sie als Virenschutz „der nächsten Generation" gelten – Schwachstellen ungeschützt lassen. Moderne Gegner haben ein Arsenal an dateilosen und nicht signaturbasierten Angriffsmethoden entwickelt und sind sehr effizient bei der Erstellung und Nutzung neuer Malware geworden – die überwiegende Mehrheit davon ist weniger als 24 Stunden alt. Im Folgenden werden wir uns ansehen, wie Sicherheitsteams ihren Ansatz zur Endpunktsicherheit weiterentwickeln können, um sich gegen diese Bedrohungen zu schützen.

Der Cybersicherheitsmarkt hat versucht, dem Bedarf an Tools gerecht zu werden, die moderne, komplexe Angriffe erkennen und es Unternehmen ermöglichen, Vorfälle zu untersuchen, ihre Ursache zu identifizieren und betroffene Endpunkte zu schützen. Für diese Tools gibt es jede Menge Kürzel, wie NGAV („Next-Generation Antivirus“), EPP („Endpoint Protection Platforms“) oder EDR („Endpoint Detection & Response“), die sich in ihrem Funktionsumfang immer häufiger auch überschneiden. Das macht es zum einen schwieriger, sich für eine Lösung zu entscheiden, zum anderen hat sich noch keine als die für Unternehmen am besten geeignete Sicherheitslösung bewährt. Laut dem Ponemon Institute haben fast 67 Prozent der Befragten das Gefühl, nicht über die Zeit und die Ressourcen zu verfügen, um alle Endpunktschwachstellen ausreichend zu patchen.[1] Tests des SANS Institutes ergaben zudem, dass EDR-Produkte in der Regel nur 26 Prozent aller Angriffsvektoren erkennen.[2] Wenn EPP keinen ausreichenden Schutz bietet und EDR Angriffe nicht abwehrt, dann kann ein Unternehmen nicht angemessen reagieren.

In diesem Whitepaper werfen wir einen Blick auf die spezifischen Funktionen, die Unternehmen benötigen, um ihre Endpunkte vor modernen Bedrohungen zu schützen. Außerdem untersuchen wir skalierbare Strategien für den Einsatz dieser Funktionen zur Optimierung von SecOps-Workflows und Sicherheitsergebnissen, heute und in Zukunft.

Gute Prävention ist nach wie vor die beste Grundlage für Sicherheit

Die Gegner sind gerissen und die Anzahl und Vielfalt potenziell anfälliger Endpunkte nimmt weiter zu. Es mag nicht möglich sein, 100 Prozent aller Bedrohungen abzuwehren – auf jeden Fall nicht, ohne auch legitime Vorgänge zu blockieren und den Geschäftsbetrieb erheblich zu stören.

Man muss sich jedoch auch im Klaren darüber sein, dass eine effektive Bedrohungserkennung und -abwehr ohne eine konsequente, koordinierte Prävention nicht machbar ist. Selbst wenn eine EDR-Lösung außergewöhnlich gut funktioniert, erkennt sie Angriffe erst, wenn der Schaden bereits verursacht wurde. Das heißt, SecOps kann nur noch reagieren, muss sich zunächst um den bereits entstandenen Schaden kümmern, diesen dann unter Zeit- und Kostenaufwand analysieren und bewerten und kann erst danach Ressourcen zur Schadensbegrenzung aufwenden. EDR ist wie ein Kollisionssensor, der einen Airbag auslöst – Airbags retten Leben, aber den Aufprall von vornherein zu verhindern, wäre noch besser. Zu einem Präventionsansatz gehört die Bereitstellung einer Sicherheitslösung, die einem Kollisionsvermeidungssensor entspricht. Der erste Schritt zu guter Prävention ist es, zu überprüfen, wie das Unternehmen mit Bedrohungen umgeht.

Die drei wichtigsten Anforderungen für den Endpunktschutz

Hacker müssen bestimmte Schritte absolvieren, um vertrauliche Daten zu stehlen, Ransomware einzuschleusen oder andere Ziele zu erreichen. Nahezu jeder Angriff beginnt mit der Infektion und Infiltration eines Endpunktes – obwohl die meisten Unternehmen in den Endpunktschutz investiert haben.

Moderne Angreifer kombinieren häufig zwei Vorgehensweisen: Ausnutzen von Sicherheitslücken und Einsatz schadhafter Dateien. Obwohl diese Methoden grundverschieden sind, können sie in verschiedenen Kombinationen eingesetzt werden, nicht nur einzeln.

- **Bei Exploits** nutzen die Kriminellen Schwachstellen im Code des Betriebssystems oder einzelner Anwendungen aus, um sich Zugang zu einem System zu verschaffen.
- **Bei Malware** handelt es sich um schädliche Dateien oder schädlichen Code. Damit können Angreifer Systeme infizieren und ausspähen, Daten stehlen und verschiedene andere Aktivitäten ausführen.
- **Ransomware** ist eine spezielle Art von Malware, die den Zugriff auf wichtige Dateien oder Daten sperrt, in der Regel durch Verschlüsselung. Der Angreifer verlangt dann ein Lösegeld für die Bereitstellung des Schlüssels für die Entschlüsselung.

Da die Funktionsweisen von Malware und Exploits fundamental verschieden sind, muss ein wirksamer Schutz beide Angriffsarten abdecken und die folgenden Funktionen umfassen.

1. Malwareanalyse

Die heutige komplexe Bedrohungslandschaft in Verbindung mit der Vielfalt, Anzahl und Komplexität der Bedrohungen in modernen Unternehmensumgebungen erschwert die wirksame Bedrohungsabwehr. Verschärft wird dieses Problem durch die Herausforderung, nie zuvor gesehene Malware und Exploits sowie schadhafte Inhalte erkennen zu müssen.

Um diesen raffinierten, zielgerichteten und verschleierten Bedrohungen zu begegnen, muss der Endpunktschutz mit gemeinsam genutzten Bedrohungsdaten trainiert werden, um Abwehrmethoden zu erlernen und weiterzuentwickeln. IDC Research berichtet, dass 39 Prozent aller Sicherheitsexperten die gemeinsame Nutzung von Bedrohungsdaten als sehr oder extrem wichtig für die Stärkung der Sicherheit einschätzen.[3] Zu diesem Zweck ermöglicht die Integration cloudbasierter Bedrohungsdaten in den Endpunktschutz eine genauere Analyse und damit eine schnellere Erkennung potenziell unbekannter Bedrohungen. Maschinelles Lernen am Endpunkt sollte es möglich machen, eine Datei schnell zu bewerten und verdächtige Merkmale sofort zu erkennen und bei Bedarf gleichzeitig eine tiefergehende Analyse durchzuführen, um auch der besten Malware auf die Schliche zu kommen.

2. Prävention gegen Ransomware

Ransomware ist zwar nicht neu, doch größere Angriffe wie WannaCry, Petya/NotPetya und TrickBot haben gezeigt, dass herkömmliche Präventionsmethoden moderner Ransomware nicht gewachsen sind. Hacker haben ihre Strategie und den Einsatz von Malware weiterentwickelt und automatisiert und arbeiten nun gezielter und außerordentlich gut getarnt.

Die Abwehr von Ransomware erfordert eine „Defense-in-Depth“-Strategie am Endpunkt, um Ransomware in den verschiedenen Phasen des Angriffszyklus zu erkennen und auszuschalten. Im Falle von WannaCry müsste die Exploit-Prävention zuerst die Angriffsmethode erkennen, die versucht, Kernelprivilegien auf die Benutzerebene zu eskalieren, und dann den Angriff blockieren. Wenn dies fehlschlägt, sollte der übergeordnete Prozess erkannt und daran gehindert werden, einen untergeordneten Prozess zu erzeugen. Wenn diese Maßnahmen nicht ausreichen, um Bedrohungen zu erkennen, sollte der Agent in der Lage sein, lokale Analysen und maschinelles Lernen zu nutzen, um die bekannten Merkmale von WannaCry zu identifizieren.

1. „Challenging State of Vulnerability Management Today: Gaps in Resources, Risk and Visibility Weaken Cybersecurity Posture“, Balbix Inc. und Ponemon Institute, Juli 2018, https://www.balbix.com/app/uploads/Ponemon-Survey-Vuln-Management-.pdf
2. „Endpoint Protection and Response: A SANS Survey“, SANS Institute, 12. Juni 2018, https://www.sans.org/reading-room/whitepapers/analyst/membership/38460
3. Konstantin Rychkov und Duncan Brown: „Bridging Security Gaps with Network-to-Endpoint Integration“, IDC Research, Oktober 2018, https://www.paloaltonetworks.com/resources/whitepapers/bridging-security-gaps-with-network-to-endpoint-integration

WastedLocker: Kombination von Malware und Exploits

Ransomware wie WastedLocker, die bereits für Lösegeldforderungen in Millionenhöhe eingesetzt wurde, nutzt eine Kombination aus Exploits, Malware und verschiedenen innovativen Funktionen, um Sicherheitsvorkehrungen an Endpunkten zu umgehen. Die Ransomware WastedLocker verleitet Websitebesucher dazu, vermeintliche Software-Updates herunterzuladen. Diese enthalten ein Cobalt Strike-Ladeprogramm, das dann die Ransomware auf das System der Benutzer herunterlädt. WastedLocker breitet sich im Netzwerk des Opfers aus und nutzt eine oder mehrere Systemmanagementfunktionen, um sicherzustellen, dass die Ransomware erfolgreich ausgeführt werden kann, bevor es sie startet.

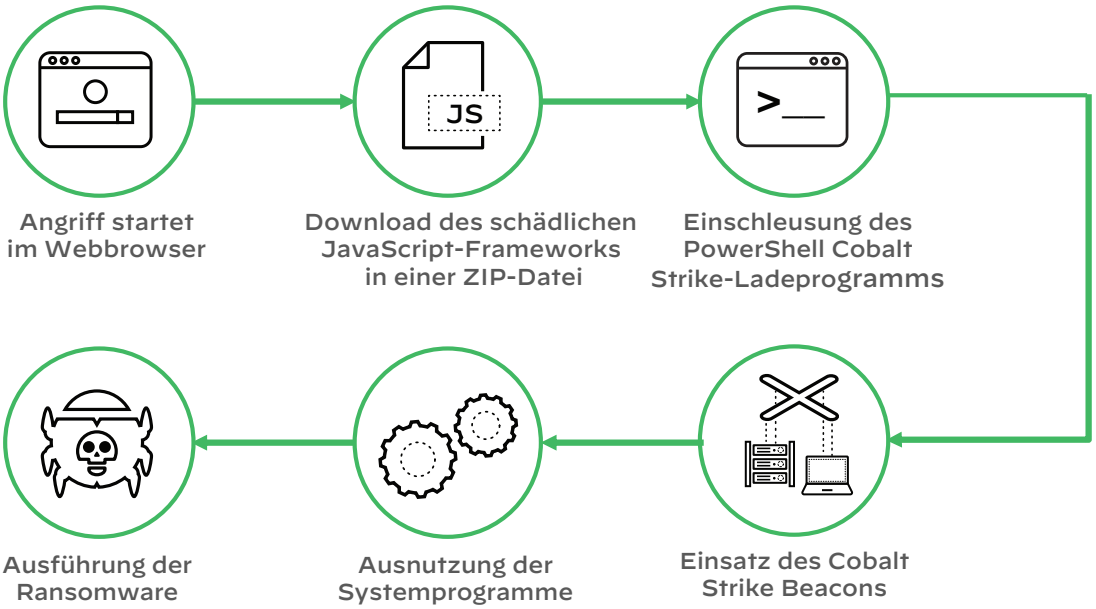

Abbildung 1: Vereinfachte WastedLocker-Angriffssequenz

3. Prävention gegen Exploits

Jedes Jahr werden Tausende von neuen Softwareschwachstellen und Sicherheitslücken entdeckt, die eine sorgfältige Bereitstellung von Softwarepatches durch die Softwarehersteller sowie Patchmanagement durch System- und Sicherheitsadministratoren in jedem Unternehmen erfordern. Die Behebung von Schwachstellen ist die wichtigste Aufgabe von Patches.

Mehr über Exploit-Methoden

Viele moderne Bedrohungen infiltrieren scheinbar harmlose Datendateien mit schadhaftem Code. Wenn diese Dateien geöffnet werden, nutzt der Code ungepatchte Schwachstellen in der nativen Anwendung, in der die Datei angezeigt wird, aus, und wird ausgeführt. Diese Art von Angriff ist möglich, wenn die betroffene Anwendung von der IT-Sicherheitsrichtlinie genehmigt wird.

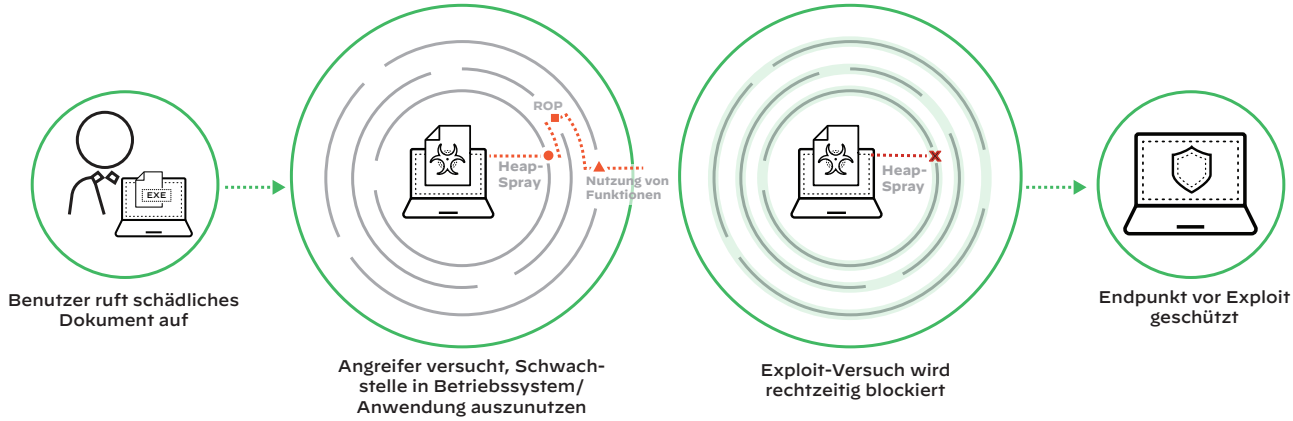

Abbildung 2: Fokus auf Exploit-Methoden, nicht auf die Exploits selbst

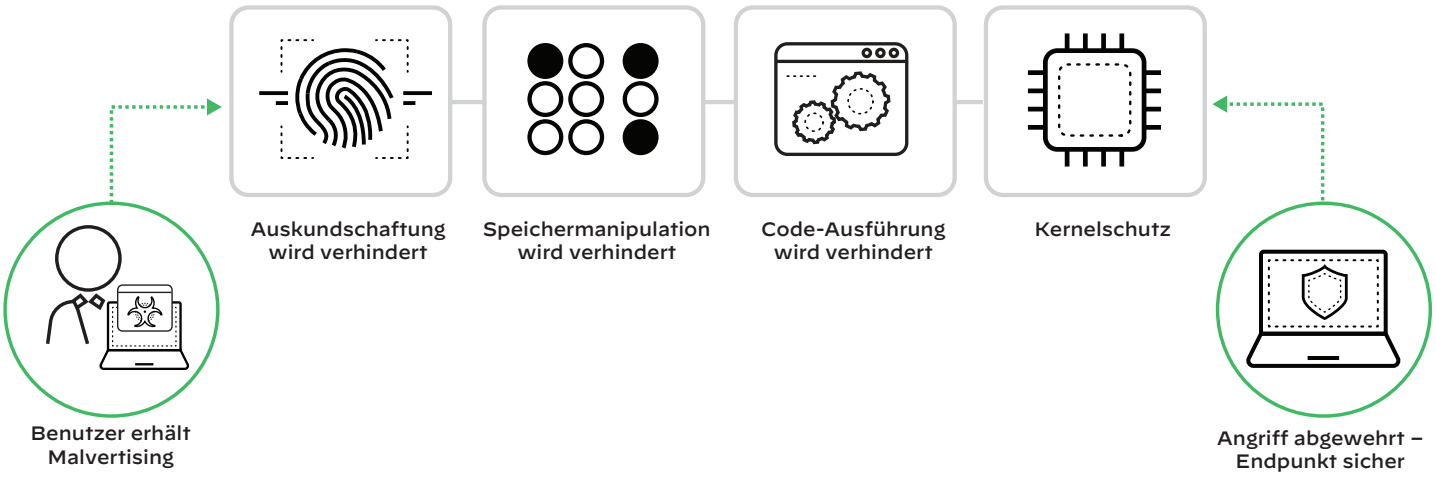

Abbildung 3: Mehrere Methoden zur Prävention gegen Exploits

Es gibt zwar Tausende Exploits, aber alle basieren auf einer kleinen Anzahl von Exploit-Techniken, die nur selten verändert werden. Unabhängig von der Sicherheitslücke oder ihrer Komplexität müssen Angreifer eine Reihe dieser Kernangriffstechniken nacheinander ausführen, um ihr Ziel zu erreichen.

Die Prävention gegen Exploits konzentriert sich auf die von allen Exploits verwendeten Kerntechniken. Indem Tools diese Techniken außer Kraft setzen, werden Anwendungsschwachstellen negiert, unabhängig davon, ob sie gepatcht werden oder nicht. Dieser Ansatz ist besonders wichtig für den Schutz heterogener Umgebungen – wie z. B. solche mit Cloud-Workloads – in denen physische Endpunktkontrollen in virtuellen Umgebungen unvorhergesehene Komplikationen verursachen können.

Eine zukunftssichere Strategie für Endpunktsicherheit

Prävention ist zwar enorm wichtig, reicht aber für sich allein nicht als Schutz vor modernen Angreifern aus. Ihre Endpunktsicherheitslösung mag 98 Prozent aller Angriffe blockieren, doch auch die restlichen 2 Prozent müssen erkannt und abgewehrt werden.

Diese Erkennungs- und Abwehrmöglichkeiten sollten einen Schritt weitergehen – Angreifer beschränken sich schließlich nicht auf Ihre Endpunkte, also sollten das Ihre Sicherheitstools auch nicht tun. Hier hat EDR versagt und oft dazu geführt, dass Sicherheitsteams Stunden damit vergeudeten, Hinweisen auf Angriffe nachzugehen, nur um herauszufinden, dass sie bereits durch eine Firewall oder einen anderen Schutzmechanismus blockiert wurden. Besser ist es, Endpunktschutz und Bedrohungserkennung als Bestandteile einer ganzheitlichen erweiterten Erkennungs- und Reaktionsplattform (XDR) einzusetzen, die maschinelles Lernen auf einen zentralisierten Datenstrom anwendet, um einen vollständigen Einblick in Angriffe über Datenquellen hinweg zu ermöglichen und die Prävention über Sicherheitspunkte hinweg zu koordinieren. XDR bietet umfassendere Präventionsfähigkeiten als jedes NGAV oder EDR und bietet die nötige Transparenz und die leistungsstarken Analysemöglichkeiten, die Sicherheitsteams brauchen, um Angreifer heute und in Zukunft zu bekämpfen.

Eine Studie von Forrester Consulting aus dem Jahr 2020 zeigt, dass nur 49 Prozent aller Unternehmen derzeit das Gefühl haben, über gut integrierte Sicherheitsinstrumente zu verfügen. Unternehmen verbringen zu viel Zeit damit, die richtigen Daten zu beschaffen und diese dann in das passende Format für die Analyse zu bringen. Häufig müssen Daten aus mehreren Quellen zusammengetragen werden, um festzustellen, welche Benutzer, Geräte, Prozesse oder Anwendungen mit bestimmten Ereignissen in Verbindung stehen. XDR automatisiert diesen Vorgang durch Alert Stitching. Dabei werden zusammengehörende Warnmeldungen aus verschiedenen Datenquellen zueinander in Beziehung gesetzt. So lässt sich die Menge der unterschiedlichen Warnmeldungen, mit denen Analysten täglich konfrontiert werden, drastisch reduzieren.

Wenn sie weniger Warnmeldungen erhalten, können Sicherheitsteams viel schneller handeln. Führende XDR-Lösungen können Sicherheitslücken durch nahtlos integrierten Endpunktschutz sowie Erkennungs- und Abwehrfunktionen mit minimalem Platzbedarf, einer cloudbasierten Verwaltungsschnittstelle und umfassender Datenerfassung für die Ereignis- und Alarmprotokollierung schließen, ohne dabei von Signaturen zur Prävention abhängig zu sein. Dadurch erhalten Sicherheitsteams die Transparenz, die sie für die Einführung präventiver Maßnahmen benötigen, ohne die Endpunktverwaltung zu beeinträchtigen.

Ihre nächste NGAV-Investition sollte in eine XDR-Lösung sein

Voneinander isolierte Tools und manuelle Prozesse haben in der Zukunft von SecOps keinen Platz. Um raffinierte Angreifer und ihr wachsendes Arsenal an Tools zu stoppen, bedarf es eines wesentlich intelligenteren und robusteren Einsatzes von Automatisierung, großen Datenmengen und maschinellem Lernen sowie eines stärker integrierten Toolkits, das eine schnellere und umfassendere Einführung neuer Funktionen ermöglicht. Investitionen in die Endpunktsicherheit sollten nicht mehr nur auf der Grundlage der Stärke des Malwareschutzes und der Größe des Endpunktagenten getätigt werden, sondern auch unter Berücksichtigung der Art und Weise, wie sie die Arbeitsabläufe von Sicherheitsoperationen erleichtern, die für den allgemeinen Sicherheitsstatus des Unternehmens von entscheidender Bedeutung sind.

Die folgenden Punkte sollten Sie in Ihre Überlegungen einbeziehen, bevor Sie in eine Sicherheitslösung investieren:

- Integrierte Schutz-, Erkennungs- und Abwehrfunktionen, die durch KI und maschinelles Lernen ermöglicht werden und Lücken automatisch schließen.
- Zentrale Steuerungsfunktionen, die eine nahtlose Kommunikation zwischen SecOps, Endpunkt- und Netzwerkadministratoren und IR-Teams ermöglichen
- Weniger, aber bessere Warnmeldungen
- Umfassende Transparenz in der gesamten Infrastruktur einschließlich Endpunkte, Netzwerk und Cloud, um die Erkennungs- und Abwehrzeiten zu verkürzen

XDR ist die einzige Endpunktsicherheitslösung, die all diese Kriterien erfüllt. Durch die Kombination aussagekräftiger Daten aus Netzwerk, Endpunkt und Cloud mit Analysefunktionen erstellt Cortex XDR automatisch von jeder Bedrohung und ihrem Ursprung ein umfassendes Bild und beschleunigt so die Identifikation und Reaktion, sodass jeder Schritt von der ersten Sichtung von Warnmeldungen bis zur proaktiven Bedrohungssuche schneller und leichter von der Hand geht. Durch die enge Verzahnung mit Sicherheitspunkten wird auch die Abwehr beschleunigt. Die gewonnenen Erkenntnisse können zur Anpassung der Verteidigung und zur effektiveren Verhinderung zukünftiger Bedrohungen verwendet werden. Darüber hinaus erfordert XDR weniger Kenntnisse von Sicherheitsanalytikern für die Reaktion auf Angriffe und senkt so die Kosten von Sicherheitsoperationen.

Fazit

Durch eine Strategie mit Schwerpunkt auf Prävention mit Integration von Schutz, Erkennung und Abwehr können Unternehmen vier grundlegende Herausforderungen besser bewältigen: unzureichende Sicherheit, zu viele Warnmeldungen, disparate Sicherheitsoperationen und die zunehmende Verweildauer von Angreifern.

Bei Ihrer nächsten Investition in die Endpunktsicherheit sollten Sie eine Reihe von Zielen vor Augen haben: integrierter Schutz, Eliminierung von Warnmeldungen, Erkennung und Abwehr in einem einfacheren Endpunktagenten, Vereinheitlichung von SecOps, Endpunktadministration und IR über fortschrittliche Kausalitätsketten und Bereitstellung vollständiger Transparenz der gesamten Infrastruktur vom Endpunkt über das Netzwerk bis zur Cloud, um die Erkennungs- und Abwehrraten zu erhöhen und letztlich die Verweildauer zu verkürzen.

paloalto NETWORKS

Oval Tower, De Entrée 99–197
1101 HE Amsterdam
Niederlande

Telefon: +31 20 888 1883

www.paloaltonetworks.de

what-is-the-next-step-for-next-gen-antivirus-wp-111220-de