

STORMSHIELD

Tipps zur Auswahl der richtigen Lösung für Endpoint Security

EDR oder HIPS: Mit welchem Ansatz lassen sich ausgereifte Cyberangriffe wirksam abwehren?

WHITEPAPER



Während das Thema Cybersicherheit immer mehr in den Mittelpunkt des Interesses rückt, bemühen sich Cyberkriminelle, unter dem Radar zu bleiben. Deshalb entwickeln sie ihre Angriffstechniken stetig weiter, und weil sie genau wissen, wie die Zahnräder ineinander greifen, versuchen sie, bösartige Tools zu entwickeln, mit denen sie die Cybersicherheitslösungen auf Workstations austricksen können.

Herkömmliche Antiviren- und andere Erkennungssysteme, insbesondere solche, die ausschließlich auf Signaturen basieren, scheinen heute von komplexen Techniken, wie dem Hijacking legitimer Anwendungen, der Ausweitung von Berechtigungen sowie im Geheimen operierender Malware, abgehängt zu werden. Aus diesem Grund werden Lösungen, die sich auf die Erkennung und Verhinderung bekannter Angriffe konzentrieren, immer unzureichender, um diese neue Generation ausgereifter und unbekannter Cyberangriffe zu bekämpfen.

Für Unternehmen ist es von entscheidender Bedeutung, ***Lösungen zu implementieren, die das Verhalten laufender Prozesse im Detail analysieren, um potenzielle Bedrohungen innerhalb des Systems zu erkennen****. Die Lösung der Wahl muss deshalb in der Lage sein, Bedrohungen proaktiv, automatisch und in Echtzeit zu identifizieren und abzuwehren, um einen möglichst reibungslosen, kontinuierlichen Geschäftsbetrieb zu gewährleisten.*

Dieses Whitepaper er läutert die verschiedenen Mechanismen, über die ein Sicherheitssystem für Workstations und Server verfügen muss, um Bedrohungen erkennen und Endgeräte effektiv schützen zu können.

Es richtet sich an Verantwortliche für die Sicherheit von Informationssystemen und gibt Ihnen Informationen an die Hand, die Sie bei der Entscheidungsfindung gemäß Ihren Bedürfnissen unterstützen können.

Inhalt

1

Cyberangriffe: Wie ist die Vorgehensweise?

2

Lösungen mit Verhaltensanalyse

3

Endpoint Detection & Response

Der perfekte Schutz?

4

Verschiedene HIPS-Schutztechniken

4.1 Regelbasierter Ansatz

4.2 Kontextbasierter Ansatz

4.3 Das „Hardening“

5

Stormshield Endpoint Security Evolution

Die Lösung zum Schutz von Workstations

01

Cyberangriffe: Ablauf

Laut ANSSI hat sich die Zahl der Opfer von Cyberangriffen zwischen 2019 und 2020 vervierfacht. Wie aus einem Bericht des französischen Senats hervorgeht[2], nutzten Cyberkriminelle günstige Gelegenheiten, sodass die Anzahl der registrierten Phishing-Angriffe im Zeitraum vom 1. bis zum 23. März 2020 um 667 % gestiegen ist.

Darüber hinaus können Systeme oder Infrastrukturen niemals zu 100 % sicher sein, auch wenn das Bewusstsein für Cybersicherheit unter Benutzern allmählich gestiegen ist. Deshalb erfinden Cyberangreifer immer wieder neue Tricks, um immer gezielter in die Informationssysteme von Unternehmen aller Größenordnungen einzudringen.

91 %

der gezielten Angriffe erfolgen über die „Spear-Phishing"-Methode

Ihr Ziel? Sensible Daten (medizinische, Bank- oder Geschäftsdaten usw.) auszuspähen, sie zu verschlüsseln, um Lösegeld zu erpressen oder die Daten zu veröffentlichen, oder sogar die Produktivität des Zielunternehmens zu beeinträchtigen (z. B. eine Händlerwebsite, Produktionslinien usw.). Dazu versuchen Cyberangreifer, in die implementierten Sicherheitssysteme einzudringen und sich darin einzunisten, indem sie beispielsweise Schwachstellen der installierten Software oder von Geräten ausnutzen.

Um besser zu verstehen, wie ein Cyberangriff funktioniert, konzentrieren wir uns auf die drei entscheidendsten Phasen, die es Angreifern ermöglichen, ihre gewünschten Ziele zu erreichen. In der Anfangsphase wird eine Benutzer-Workstation oder ein exponierter Service als Einfallstor genutzt, sodass Cyberkriminelle einen ersten unprivilegierten Zugriff auf das System erhalten. In der zweiten Phase versuchen die Angreifer dann, tief in das Informationssystem einzudringen, indem sie sich beispielsweise Zugang zu einem privilegierten Konto verschaffen oder andere Maschinen infizieren. In Phase drei lösen sie die bösartige Aktion als solche aus: Verschlüsselung, Datendiebstahl…

Im Folgenden gehen wir genauer auf diese drei Phasen ein.

[2] http://www.senat.fr/rap/r20-678/r20-678_mono.html

PHASE 1

INFORMATIONS-SAMMLUNG UND ERSTINFEKTION



Zunächst suchen Cyberkriminellen nach potenziellen Opfer innerhalb eines Zielunternehmens, um Angriffsvektoren zu implementieren, die menschlicher und/oder technologischer Art sein können.

Auf menschlicher Ebene nutzen Angreifer Techniken des Social Engineering (LinkedIn, Facebook usw.), um Informationen zu sammeln, mit denen sie die Person(en) ablenken können, die für die Erstinfektion ausgewählt wurden.

So versuchen sie, Empfänger zu täuschen, damit sie einen Anhang öffnen oder auf einen schädlichen Weblink klicken – eine Technik, die für ihre Wirksamkeit bekannt ist: 91 % der gezielten Angriffe[2] erfolgen über diese „Spear-Phishing"-Methode (gezieltes Phishing).

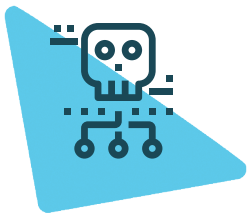
Ein Manöver zur Ablenkung der Wachsamkeit kann beispielsweise darin bestehen, dass Cyberangreifer die Identität eines Absenders (Finanzinstitut, Lieferant usw.) annehmen, welcher der Zielperson bekannt ist.

Auf technologischer Ebene versuchen Cyberkriminelle, Lücken im Sicherheitssystem auszunutzen. Sie profitieren dabei von Systemen, die nicht ausreichend geschützt sind, wie z. B. RDP-Server mit Zugriffsmöglichkeit über das Internet. Möglicherweise versuchen sie auch, die Schwachstellen von anfälligen und nicht aktualisierten Anwendungen auszunutzen. BEISPIELSWEISE veröffentlichte das Canadian Cybersecurity Center[3] im März 2021 eine Warnung und empfahl mehrere Updates, um die aktive Ausnutzung von Schwachstellen im Zusammenhang mit Microsoft Exchange zu verhindern.

Das Ziel: Schadcode ausführen, um ein Programm auf der Zielmaschine zu installieren, das die Infiltration durch Cyberangreifer ermöglicht.

[2] http://www.itpronews.fr/3648/2012/12/spear-phishing-plus-de-90-des-attaques-ciblees.html

[3] https://cyber.gc.ca/fr/avis/exploitation-active-des-vulnerabilites-de-microsoft-exchange



PHASE 2

LATERALISIERUNG UND AUSWEITUNG

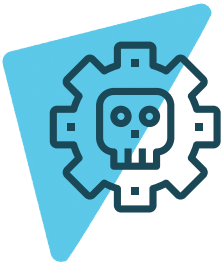
Nachdem die Phase der Erstinfektion abgeschlossen ist, versuchen Angreifer, das Netzwerk zu scannen, um sich einen besseren Überblick zu verschaffen. In dieser Lateralisierungsphase möchten sie tiefer in das Informationssystem eindringen, um die Maschinen und Benutzer- oder Administratorkonten zu identifizieren, die ihnen dabei helfen können, ihre Ziele zu erreichen.

Sie werden also zunächst durch verschiedene Systeme und Konten navigieren und diese häufig wechseln. Möglicherweise installieren sie auch eigene Tools aus der Ferne, um Schwachstellen im System auszunutzen und Anmeldedaten zu erbeuten.

Das Ziel: Sich tief in der Infrastruktur einzunisten, um gezielt Maschinen zu finden, auf denen der Angriff die größten Auswirkungen entfalten kann.

Anschließend versuchen sie, tief in das System einzudringen, was der Ausweitungsphase entspricht. Sie geben sich oft als autorisierte Benutzer aus, was sehr schwierig zu erkennen ist. Dazu können sie eine Privilegienerhöhung durchführen, um als lokaler Administrator aufzutreten, oder sie übernehmen die Kontrolle über ein Benutzerkonto mit Zugriff auf eine bestimmte Software. Außerdem kombinieren sie mehrere Angriffsvektoren, um auch andere anfällige Maschinen zu infizieren.

Gängige Vorgehensweisen sind dabei, Schwächen, Fehlkonfigurationen der Infrastruktur oder bestehende Schwachstellen auszunutzen. Ein Beispiel hierfür wäre eine mangelhafte Segmentierung innerhalb eines Unternehmensnetzwerks, die den Zugriff auf für Angreifer interessante Systeme, wie einen Server mit sensiblen Daten, ermöglicht.



PHASE 3

AUSWIRKUNGEN

Diese dritte Phase bildet den Höhepunkt des Angriffs, bei dem Cyberkriminelle Aktionen im Einklang mit ihrem Ziel durchführen. Bei einem aktiven Cyberangriff können **Daten ausgespäht/gestohlen, Geschäftsprozesse manipuliert oder Server heruntergefahren werden**, die für das reibungslose Funktionieren des Unternehmens wichtig sind.

In dieser Phase achten Angreifer mitunter auch darauf, unerkannt zu bleiben, um das System zu einem späteren Zeitpunkt erneut auszunutzen oder einen (mehr oder weniger starken) Angriff zu starten, wie ihn TV5 Monde[4] im Jahr 2015 erlitt.

Zu beachten ist auch, dass Angreifer in manchen Fällen versuchen, die verschiedenen Datensicherungen sowie die Spuren ihrer bösartigen Aktivitäten zu löschen.

Das Ziel: Die Infrastruktur zu beschädigen, um eine für die Produktionsabläufe des Unternehmens notwendige Komponente zu blockieren. Auch Diebstahl von Daten zwecks Weiterverkauf und/oder Veröffentlichung (z. B. Gesundheitsdaten im Dark Web) oder Verschlüsselung, um ein Lösegeld vom Zielunternehmen zu erpressen.

[4] https://www.lemonde.fr/pixels/article/2017/06/10/le-piratage-de-tv5-monde-vu-de-l-interieur_5142046_4408996.html

02

Verhaltensanalysen in Lösungen

Cyberkriminelle nutzen Angriffstechniken insbesondere dazu, um unter dem Radar zu bleiben und zu verhindern, dass ihr Schadcode von den verschiedenen Sicherheitslösungen erkannt wird. **Die Erkennung von verdächtigem Verhalten sowie die präventive Unterbindung von potenziell gefährlichen Aktivitäten sind also unerlässlich.**

Deshalb ermöglicht ein *Host Intrusion Prevention System* (HIPS) den Schutz von Workstations und Servern vor Malware, indem es verdächtige Aktivitäten blockiert, die Auswirkungen auf die Systeme innerhalb einer Infrastruktur haben können.

„Manche Intrusion-Prevention-Systeme ermöglichen es Benutzern, Protokolle bösartiger Aktivitäten sowie verdächtige Codefragmente zur Analyse und möglichen Identifizierung direkt an den Hersteller zu senden. “

Stephen J. Bigelow

Senior Technology Editor

Quelle: Techtarget

Im Folgenden werden wir auf die wichtigsten Aspekte der verschiedenen Typen von HIPS-Systemen und ihre Eignung für verschiedene Anforderungen eingehen.

HIPS **auf der Basis von Signaturen**

Sie nutzen **Kenntnisse über die Schwachstellen einer Anwendung sowie bekannte Bedrohungen** und blockieren diesbezügliche Angriffe. Sie basieren auf einer Datenbank, die regelmäßig aktualisiert werden muss.

Sie identifizieren bekannte Angriffe. Allerdings können sie unbekannte oder Zero-Day-Angriffe **nicht erkennen**. Sie sind **nur bedingt für Einsatzszenarien geeignet, in denen Workstations vom Update-Server getrennt** werden müssen.

Nur wenige Optionen in der Software vorhanden.

HIPS **auf der Basis von Verhaltensanalysen**

Blockierung bekannter sowie Zero-Day-Angriffe in Echtzeit: Erkennung verdächtiger Aktivitäten legitimer Anwendungen und Prozesse ohne den Einsatz von Signaturdatenbanken oder Anwendungsanomalien

Einige HIPS-Lösungen kombinieren **verhaltensbasierte und heuristische Methoden, Speicherschutz oder sogar eine Härtung des Betriebssystems**, um einen besseren Schutz vor Bedrohungen zu gewährleisten.

Hohes Maß an Parameter- oder Regeleinstellungen und Filter, die sich an verschiedene Organisationen anpassen können.

*„Eine verhaltensbasierte HIPS-Lösung erkennt und blockiert **gängige und ausgeklügelte Angriffstechniken**, wie das Ausnutzen von Schwachstellen in Anwendungen, um einen **wirksamen Schutz des Endgeräts zu gewährleisten.** “*

Edouard Simpère
Zuständig für Endgerätesicherheit bei Stormshield

EDR oder „Endpoint Detection & Response“[5] sind Softwareprogramme, die bekannte und unbekannte Bedrohungen erkennen und abwehren, ohne auf Patches oder Updates angewiesen zu sein. Diese Systeme sind in den letzten Jahren zu einem allgegenwärtigen Begriff in der Cybersicherheit geworden. Sie bestehen üblicherweise aus Agenten, die an den verschiedenen Endpunkten eines Netzwerks eingesetzt werden, z. B. auf Workstations, Mobiltelefonen oder verschiedenen Servern innerhalb einer Infrastruktur.

Eines der allgemeinen Merkmale von EDR-Programmen ist die **kontinuierliche Überwachung von Endpunkten**. Darüber hinaus umfassen einige Lösungen auch EPP-Bausteine, um Echtzeitschutz zu bieten. Diese Funktion bildet eine erste wirksame Barriere zum Schutz vor den meisten bekannten Angriffen und einigen unbekannten Bedrohungen.

Endpoint Detection & Response: Der perfekte Schutz?

Wie ANSSI betont[6], verfügen diese Lösungen, die große Datenmengen verwalten, in der Regel über Funktionen zur **Erkennung** (von verdächtigen Verhaltensweisen legitimer Anwendungen, *nicht auf Dateien basierender Angriffe*[7]),**Untersuchung** (d.h. vollständige Visualisierung des erkannten Angriffs) und **Behebung** (Wiederherstellung von Dateien usw.).

Aus diesem Grund ergänzen EDR-Lösungen heute häufig traditionelle Lösungen, die hauptsächlich auf Signaturdatenbanken basieren. Sie bieten einen **umfassenden Einblick** und erkennen in der Regel Fälle von anormalem Verhalten legitimer Prozesse. In Folge dieser Erkennung implementiert die Lösung Maßnahmen, um den Angriff zu unterbrechen, indem sie den bösartigen Prozess stoppt. Zusätzlich werden die Systemadministratoren auf mehr oder weniger automatisierte Weise gewarnt. Diese können dann eine Maßnahme einleiten oder die EDR-Lösung kann diese automatisch und nahezu in Echtzeit umsetzen (dies hängt von der verwendeten Lösung ab). Dank dieser Funktionen können Ransomware und polymorphe Angriffe mithilfe dieser Tools erkannt und abgewehrt werden.

[5] https://www.ssi.gouv.fr/uploads/2021/06/anssi-france_relance-edr.pdf

[6] https://www.ssi.gouv.fr/uploads/2021/06/anssi-france_relance-edr.pdf

[7] https://www.riskinsight-wavestone.com/2018/10/fileless-attack-le-retour-a-la-terre/

Im Hinblick auf die Verwaltung können sie in die SIEM-Lösung eines Unternehmens integriert werden, um die erforderlichen Protokolle zu erstellen, welche die SOC-Analysten dabei unterstützen, die Suche nach Angriffen so effizient wie möglich zu gestalten.

Die meisten EDR-Lösungen auf dem Markt verfolgen heute einen *Cloud-only*- oder *Cloud-first*[8]-Ansatz, um die Datensammlung zu zentralisieren und Frühwarnzeichen oder Kompromittierungen, die auf einen Angriff hindeuten können, zu analysieren. Denn die Cloud eignet sich besonders für solche massive Sammlungen sowie die Verarbeitung und Analyse großer Datenmengen.

Allerdings kann diese Möglichkeit in einigen Anwendungsfällen angesichts der Sensibilität der zu verarbeitenden Daten nicht in Betracht gezogen werden. In solchen Fällen kann der ***On-Premise-Modus* in sensiblen Umgebungen** (Verteidigung, Ministerien, Industrie usw.) eine wirksame Option darstellen. Außerdem ist es wichtig, zwischen dem Schutzniveau zu unterscheiden, das entweder durch den Server oder durch einen auf dem Rechner installierten Client erzeugt wird.

Lassen Sie uns die wichtigsten Unterschiede zwischen den beiden Ansätzen betrachten:

Server-basierter Schutz

Bei diesem Ansatz meldet ein auf der Workstation installierter light Agent **alle Informationen an den Server** – er verfügt über keine erweiterten Funktionen.

Der Server, ob vor Ort oder in der Cloud, analysiert die Protokolle des Agenten auf bösartiges Verhalten, Anomalien auf einer bestimmten Workstation usw.

Ein light Agent benötigt **eine ständige Verbindung, um Informationen hochzuladen**. Es kann eine gewisse Latenz bezüglich der erhaltenen Antwort auftreten.

Agentenbasierter Schutz

Der Agent auf der Workstation kann **selbstständig Entscheidungen treffen** und die Workstation schützen, ohne auf seinen Server zugreifen zu müssen.

Der Server verfügt über eine geringere globale Sichtbarkeit unter Berücksichtigung der **erweiterten Funktionen des Agenten** zum Schutz der Workstation vor Malware.

Der Agent **arbeitet unabhängig und blockiert bösartige Verhaltensweisen in Echtzeit**.

Um also jederzeit einen bestmöglichen Schutz zu gewährleisten, **sollten Sie Lösungen wählen, die Malware auch ohne Netzwerkverbindung erkennen können, um einen zuverlässigen Echtzeitschutz für Workstations zu erzielen.**

[8] https://www.pcpresse.com/wp-content/uploads/2020/10/LINFO-CR01_MD.pdf

04

Verschiedene Schutztechniken HIPS

Cyberkriminelle sind sich bewusst, dass ihre Angriffe keine Aufmerksamkeit erregen dürfen, wenn sie unbemerkt bleiben möchten (Phase 2: Lateralisierung und Ausweitung). Dazu versuchen sie stetig, neue Fähigkeiten zu entwickeln, indem sie neue Taktiken und Angriffstechniken einsetzen, um herkömmliche Schutzmaßnahmen zu umgehen.

Im Folgenden gehen wir auf die wichtigsten Techniken ein und erläutern, wie Angreifer versuchen, die verschiedenen Sicherheitsvorkehrungen auszuhebeln.

255 %

Diese Zahl entspricht laut einer Studie des ANSSI dem Anstieg der Ransomware-Meldungen im Jahr 2020.

In der folgenden Tabelle werden verschiedene Angriffstechniken in den drei Phasen während eines Cyberangriffs beschrieben. Zur Erinnerung: In der dritten Phase haben die Cyberkriminellen bereits die Kontrolle übernommen und führen den eigentlichen Angriff aus, wie z. B.: Abhören oder Datendiebstahl. Dabei ist zu beachten, dass solche Prozesse oft nur schwierig zu erkennen sind, da die Angreifer auf *den ersten Blick* legitime Werkzeuge und Anmeldungen verwenden.

Phase	Techniken	Wie setzen Angreifer diese ein?	Auswirkungen
Phase 1: Entdeckung und Erstinfektion	Buffer Overflow. Beispiel: - Stack Pivot	Angreifer verursachen einen Buffer Overflow, indem sie falsch formatierte Eingabedaten bereitstellen, um die Zielanwendung dazu zu bringen, Daten über die normale Begrenzung hinaus in den Speicher zu schreiben. Auf diese Weise werden die richtigen Daten überschrieben und die Angreifer können die Kontrolle über den Ausführungsablauf der Anwendung übernehmen.	Der Code, den die Angreifer in die Zielanwendung einfügen, gibt ihnen die Möglichkeit, aus der Ferne zuzugreifen und/oder weitere bösartige Dateien (Payload) herunterzuladen und auszuführen.
Phase 1: Entdeckung und Erstinfektion	Packing Malware	Bei dieser Technik wird verhindert, dass die bösartige Datei von Sicherheitslösungen analysiert wird, indem alle Funktionen dynamisch geladen werden.	Packer erschweren die Aufgabe von Sicherheitsteams, die Malware zu identifizieren, und erhöhen die Dauer der Analyse. Außerdem können signaturbasierte Lösungen durch das Packen einer Datei umgangen werden.
Phase 1: Entdeckung und Erstinfektion	Process Hollowing. Beispiele: - RunPE - Doppelgänging	Das Prinzip besteht darin, ein System dazu zu bringen, bösartigen Code auszuführen, indem dieser als legitimer Prozess getarnt wird. Während die RunPE-Technik die Schwachstellen des Systems zum Laden von ausführbarem Code ausnutzt, bedient sich das „Doppelgänging"-Verfahren des NTFS-Transaktionsmechanismus.	Mittels Process Hollowing können Angreifer unter dem Radar von Sicherheitslösungen bleiben, die in der Regel die legitimen Systemprozesse, als die sich Angreifer ausgeben, ignorieren.
Phase 2: Lateralisierung und Ausweitung	Ausweitung von Berechtigungen Beispiele: - DLL-Hijacking - Manipulation von Access-Token	Hierbei versuchen Angreifer, sich auf einer Workstation oder einem System Zugriff auf höherer Ebene zu verschaffen, um ihre Ziele zu erreichen. Beim sogenannten DLL-Hijacking manipulieren Cyberkriminelle eine Anwendung mit hohen Privilegien, indem sie diese dazu bringen, eine manipulierte DLL zu laden. Eine andere Technik umfasst die Manipulation von Access-Token. Angreifer können Access-Token stehlen oder duplizieren, um den Ausführungskontext der Zielanwendung zu verändern und sich so zusätzliche Berechtigungen zu verschaffen.	Nach Erlangung hoher Privilegien (Administrator- oder Systemberechtigungen) lassen die Angreifer sich nur noch schwer stoppen, da sie einen großen Einfluss auf das Zielsystem nehmen können. Solche umfangreiche Berechtigungen erleichtern die Lateralisierung eines Angriffs, dies kann in einigen Fällen jedoch auch ohne spezielle Berechtigungen möglich sein.
Phase 2: Lateralisierung und Ausweitung	Pass the Hash	Bei dieser Methode stehlen Angreifer einen Hash, der zur Identifizierung eines privilegierteren Kontos dient, das potenziell zum Einloggen auf anderen Systemen verwendet wird.	So können sie sich mit dieser gestohlenen Identität auf anderen Workstations authentifizieren. Das Ziel besteht darin, neue Maschinen zu infizieren.
Phase 2: Lateralisierung und Ausweitung	Ausspähen eines Netzwerks über die Kommandozeile	Hierbei nutzen Angreifer Befehle (wie „netdiscover"), um Workstations in einem Netzwerk zu erkennen.	Auf diese Weise können sie sich einen vollständigen Überblick über die verschiedenen eingerichteten Netzwerke verschaffen.
Phase 3: Auswirkungen	Verschlüsselung von Daten	Cyberkriminelle verschlüsseln Daten, die auf Systemen (Workstations und Servern) gespeichert sind, um sie für das Opfer unzugänglich zu machen. Dazu verwenden sie in der Regel legitime kryptografische Techniken im Zusammenhang mit Windows-APIs.	Diese Technik wird insbesondere bei Ransomware-Angriffen eingesetzt, bei denen die Angreifer ein Lösegeld für die Wiederherstellung der Daten erpressen.

4.1

Regelbasierter Ansatz: eine effektive Methode

Es gibt eine Reihe von Lösungen, die auf Regeln basierende Erkennungsprozesse auf Workstations ausführen. Bei manchen Lösungen ist es für Administratoren jedoch nicht möglich, auf diese zuzugreifen. Zwar ist die Implementierung dieser Regeln relativ einfach, aber sie können sich nicht an unterschiedliche Geschäftszwecke mit speziellen Sicherheitsanforderungen anpassen.

Andere Lösungen hingegen bieten gewisse Möglichkeiten zur Einstellung von Parametern, um sich bestmöglich an das jeweilige Einsatzgebiet anzupassen. So können Benutzer neben den vom Sicherheitsanbieter vorgesehenen Regeln auch solche integrieren, die sich nach der Position, der Branche usw. richten.

Einige HIPS-Systeme kombinieren mehrere Schutztechniken, die in Form von Parametern oder Regeln – der „Sicherheitsrichtlinie der Lösung“ – zusammengestellt werden. Solche Richtlinien können von Administrator an den zu schützenden Geschäftsprozess angepasst werden. Bei einigen Lösungen können die verschiedenen Einstellungen oder Regeln individuell angepasst werden, sodass sie besser auf das jeweilige Unternehmen zugeschnitten werden können und einen höheren Schutz bieten.

Wussten Sie schon?

Die auf Agentenseite angewendeten Verhaltensregeln bieten einen sofortigen Schutz der Workstation, um die Auswirkungen eines Angriffs zu begrenzen.

Granularität der verwendeten Schutzlösungen

Einige Lösungen bieten vordefinierte und durch Administratoren erweiterbare Regellisten zur Abwehr von Malware.

Wie oben beschrieben, sollten Sie HIPS-Lösungen bevorzugen**, die konfigurierbare und sehr feine Regelsätze bereitstellen, um alle Aktionen auf Workstations zu steuern,** wie beispielsweise die Überwachung laufender Prozesse, Registrierungsdateien und -schlüssel, die Ausweitung von Berechtigungen usw.

Diese Granularität bietet den Administratoren der Organisation eine sehr hohe Anpassungsfähigkeit und generell die Möglichkeit, eine Sicherheitsrichtlinie zu implementieren, welche die Bedürfnisse und Anforderungen des Unternehmens am besten erfüllt.

Generell sollten Workstations oder Server je nach ihrem Kontext (z. B. ob sie außerhalb oder innerhalb des Unternehmensnetzwerks liegen) und dem Grad ihrer Gefährdung durch Bedrohungen betrachtet werden.

4.2 Kontextbasierter Ansatz: ein besseres Verständnis der Umgebung

Da jede Organisation eine einzigartige Konfiguration aufweist und spezifische Anforderungen hat, muss sich die Sicherheitslösung an die verschiedenen Anwendungsfälle innerhalb des Unternehmens anpassen können. Aus diesem Grund muss der gewählte Schutz von Workstations und Servern **an dem jeweiligen Nutzungskontext ausgerichtet sein und verschiedene Mobilitätsszenarien berücksichtigen**. Dazu zählt beispielsweise die Verwaltung zulässiger WLAN-Netzwerke und deren Deaktivierung, wenn eine LAN-Verbindung aktiv ist, oder das Blockieren aller anderen Verbindungen, die nicht über ein VPN erfolgen, um Bounceback-Angriffe zu verhindern.

Die Einrichtung und Nutzung einer Sicherheitslösung für Workstations erfordert deshalb eine dynamische Sicherheitsrichtlinie. Das heißt, die Lösung muss **wissen, wo sich die jeweilige Workstation befindet, und ihre Sicherheit speziell an die Umgebung anpassen**.

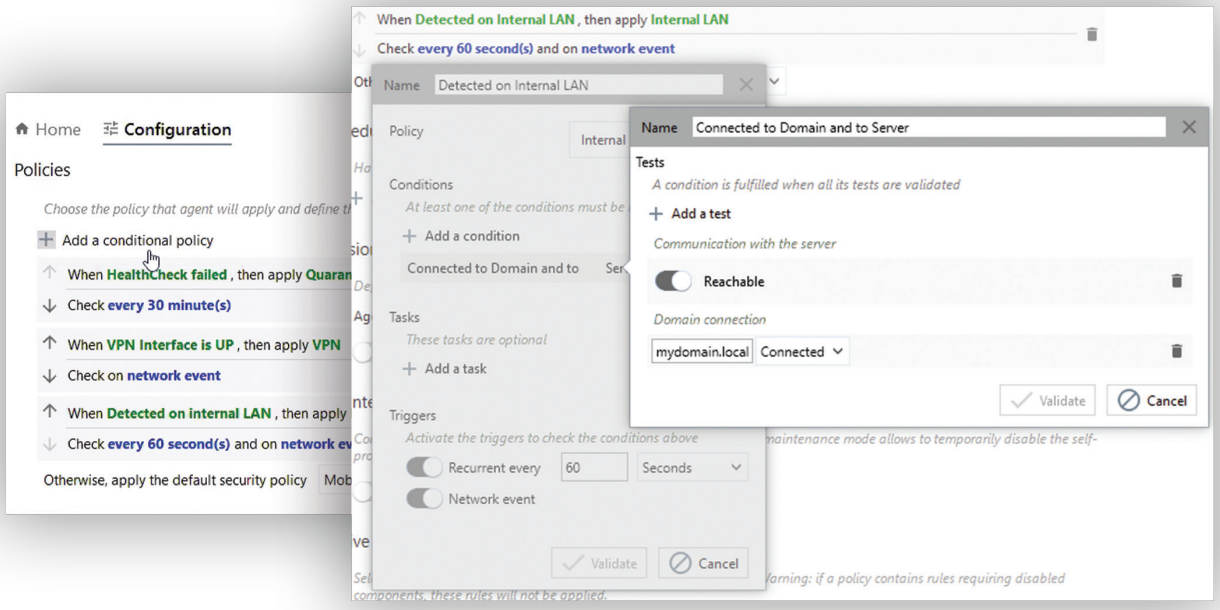


Abbildung 1

Endpoint Security mit verschiedenen Sicherheitsrichtlinien

4.3
Das „Hardening“ zum Schutz des eigentlichen Systems

Sicherheitslösungen bilden ein beliebtes Angriffsziel für Cyberkriminelle: Sie versuchen, den Schutz zu deaktivieren oder die privilegierten Berechtigungen dieser Lösungen missbräuchlich zu nutzen. Im Übrigen muss, wie das ANSSI[9] betont, die Software (und Hardware) einer Infrastruktur vor ihrem Einsatz überprüft und ihre Konfiguration gehärtet werden.

Und nicht zuletzt sollte auch die mögliche Angriffsfläche berücksichtigt werden. Experten sind sich einig, dass jede neue Komponente (Hardware oder Software), die zu einer Infrastruktur hinzugefügt wird, das Risiko erhöht, dass ein Bug oder eine Schwachstelle im Zusammenhang mit dieser Komponente vorliegt, die durch Cyberangreifer ausgenutzt werden können.

Um die Angriffsfläche zu begrenzen und den Schutz von Endgeräten zu erhöhen, werden einige Lösungen für Endpunktsicherheit gemäß dem Ansatz *Security by Design*[10] entwickelt. Das sind Lösungen, bei denen die Sicherheit und die damit verbundenen Risiken bereits bei der Produktentwicklung einbezogen und untersucht werden.

Cyberangriff bei Mitsubishi Electric[11]

Der japanische Autohersteller gab bekannt, dass er im Juni 2019 einen Cyberangriff erlitten hatte. Gemäß den Erkenntnissen einer mehrmonatigen Untersuchung hätten sich die Angreifer Zugang zum internen Netzwerk des Unternehmens verschafft und 200 MB sensible Dateien von Tausenden Mitarbeitern sowie vertrauliche technische Informationen gestohlen.

Wie kam es dazu?

Eine aus China stammende Cyberkriminellengruppe soll eine Zero-Day-Lücke im Antivirenprogramm des Unternehmens ausgenutzt haben, um schädliche Dateien zu installieren. Laut dem Hersteller der gehackten Software hätten die Angreifer eine Schwachstelle in Form eines Verzeichniswechsels ausgenutzt, um Dateien aus einer beliebigen Zip-Datei in einen bestimmten Ordner auf dem Antiviren-Server zu extrahieren. Dies hätte zu einer Ausführung von Code aus der Ferne (*Remote Code Execution*) geführt.

[9] https://www.ssi.gouv.fr/uploads/2020/08/anssi-guide-recommandations_architectures_systemes_information_sensibles_ou_diffusion_restreinte-v1.1.pdf

[10] https://www.securecontrolsframework.com/security-privacy-design-principles

[11] https://www.zdnet.fr/actualites/une-faille-0day-de-l-antivirus-trend-micro-utilisee-dans-le-piratage-de-mitsubishi-electric-39898077.htm

Dazu muss die allgemeine Architektur solcher Lösungen gemäß den Regeln der defensiven Softwareprogrammierung um eine sichere Microservice-Architektur herum entwickelt werden. Insbesondere in diesem Aspekt gilt das Prinzip des geringsten Privilegs.

Auf diese Weise kann die Lösung in **mehrere unabhängige Services** unterteilt werden, die maximale Sicherheit garantieren, indem jedem Benutzer eine bestimmte Rolle mit eingeschränkten Berechtigungen zugewiesen wird. So darf z. B. das Modul, das die Verbindung zum Konfigurationsserver verwaltet, nicht gleichzeitig auch für die Interpretation dieser Daten zuständig sein. Oder der Service, der Protokolle verwaltet, beschäftigt sich ausschließlich mit dieser Aufgabe und kann nicht auf die zugrunde liegende Sicherheitsrichtlinie zugreifen.



Abbildung 2
Sicherheitslösung, die in mehrere unabhängige Services unterteilt ist

Um ein hohes Maß an Robustheit zu erreichen, müssen die Prozesse zum Aufbau der Sicherheitssoftware auch strenge Coding-Regeln festlegen und die Verwendung verschiedener Kompilier- und Ausführungsoptionen umfassen. Diese Optionen begrenzen das Risiko der Ausnutzung von Bugs sowie die Anzahl der Fehler, indem vor und während der Ausführung mehr Kontrollen ausgeführt werden.

Zusammenfassend lässt sich sagen, dass **gehärtete oder robuste Lösungen, die auf diesen Prinzipien basieren, einen besseren Schutz vor Cyberangriffen bieten**.

Stormshield Endpoint Security Evolution: die Lösung zum Schutz von Workstations

Stormshield Endpoint Security Evolution **schützt sensible Umgebungen** indem sie Angriffe in einem frühen Stadium abwehrt, bevor sie sich auf Ihre Umgebungen auswirken können.



Erweiterte Verhaltensanalyse , die unbekannte Bedrohungen, Zero-Day-Angriffe und *Fileless*-Angriffe abwehren kann.



Eigenständige Lösung , die ohne Netzwerkverbindung funktioniert, um das Sicherheitsniveau von Endpunkten aufrechtzuerhalten.



Erweiterte Gerätekontrolle. Breites Spektrum an Gerätekontrollen: Überprüfung von WLAN-Netzwerken und USB-Sticks, Datenträgerzugriff oder Netzwerkverbindungen.



91 %

der gezielten Angriffe erfolgen über die „Spear-Phishing"-Methode

40 %

der Erstinfektionen nutzen die „Process-Hollowing"-Technik

255 %-iger

Anstieg der Meldungen von Ransomware im Jahr 2020 (laut einer Studie des ANSSI)

EINIGE BEISPIELE FÜR EINEN ANGRIFF

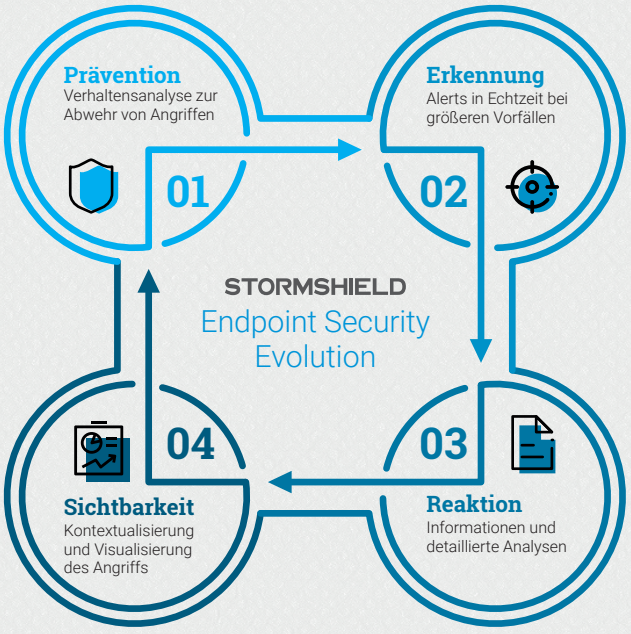


EINIGE UNVERZICHTBARE TIPPS

Hüten Sie sich vor verdächtigen E-Mails mit Anhängen oder vor zweifelhaften Websites.

Führen Sie regelmäßig Sicherungen durch.

Aktualisieren Sie Ihre Anwendungen, Plug-ins und Betriebssysteme.



DIE **EUROPÄISCHE WAHL** FÜR **CYBERSICHERHEIT**

www.stormshield.com

Jegliche Verbreitung, Vervielfältigung oder Präsentation dieses Whitepapers, auch auszugsweise, auf einem beliebigen Datenträger zu anderen Zwecken als zur privaten Nutzung ist untersagt und kann zivil- und strafrechtliche Folgen für die Person nach sich ziehen, die dieses Verbot missachtet.

Copyright © 2022 Stormshield