MEINUNGEN

WORKSTATIONS: EINTAUCHEN IN DIE WELT DES VERDÄCHTIGEN VERHALTENS

Adrien Brochot
Product Manager,
Stormshield

Verdächtiges Verhalten zu definieren, kann aufgrund der Komplexität des Themas schwierig sein. Unabhängig davon, ob Benutzer, Anwendungen oder sogar Codezeilen ursächlich sind, müssen derartige Auffälligkeiten auf Workstations untersucht werden, um die digitale Sicherheit von Unternehmen zu gewährleisten. Die Gründe werden nachfolgend erläutert.

Mit dem Aufkommen von „*Bring Your Own Device*“ (BYOD), der sogenannten Schatten-IT und der Verbreitung von Telearbeit wird die IT-Sicherheit in Unternehmen stark auf die Probe gestellt. Cyberbedrohungen in der Arbeitswelt sind zahlreich, und die Workstations der Mitarbeiter gehören zu den Schwerpunkten, die bei IT-Sicherheitsverfahren berücksichtigt werden müssen. Zu diesem Zweck müssen sie sorgfältig unter die Lupe genommen werden. Der Zugriff auf Dateien, Register, Netzwerke und Anwendungen ist genau wie die Tausenden oder sogar Millionen von Aktionen, die täglich auf den Workstations durchgeführt werden, alles andere als gewöhnlich, da sie jeweils in Beziehung zu einem bestimmten Kontext oder einer speziellen Aktivität stehen. Die Beobachtung, Kontextualisierung und Analyse dieser Aktionen erlauben die Unterscheidung zwischen verdächtigem Verhalten und legitimer Workstation-Nutzung und eine passende Reaktion darauf.accordingly.

WIE DEFINIEREN SIE VERDÄCHTIGES VERHALTEN?

Was ist verdächtiges Verhalten? Auf einer Workstation kann es als etwas definiert werden, das ohne Wissen des Benutzers ausgeführt wird, um böswillige Aktionen auszuführen. Verdächtiges menschliches Verhalten wäre derweil beispielsweise eine ungewöhnliche Verbindungszeit, etwa mitten in der Nacht, oder die Tatsache, dass ein Benutzer plötzlich eine Verbindung zu seiner Workstation von unterwegs herstellt. Verdächtiges technisches Verhalten kann wiederum als Anomalie auf der Workstation definiert werden. Wir unterscheiden dabei mehrere Hauptkategorien. Zunächst wäre da Software, die ohne Wissen der IT-Abteilung installiert ist. Dies könnte auf Schatten-IT hinweisen. Dann gibt es die Fälle, die unzweifelhaft Bösartiges im Sinn haben und sich deutlich von normalen Anwendungen unterscheiden. Beispielhaft sei hier Ransomware zu nennen, die nach ihrer Platzierung auf einer Workstation schnell damit beginnt, Sicherungen zu löschen und Dateien zu verschlüsseln. Eine andere Art verdächtigen Verhaltens, die manchmal beobachtet wird, ist die Übernahme normaler Funktionsweisen einer Software, um den Anwender in die Irre zu führen. Dies geschieht subtiler als bei einem eindeutig böswilligen Verhalten und kommt vor allem beim Phishing zum Einsatz. Schließlich kann verdächtiges Verhalten auch als eine Kette eigentlich gewöhnlicher Aktionen definiert werden, die unscheinbar ausgeführt werden, bevor sie erkannt werden können. Dies ist insbesondere bei APTs („*Advanced Persistent Threats*“) der Fall.

"Das Definieren von verdächtigem Verhalten dient dem Verständnis, was man erkennen muss."

Thierry Franzetti, technischer Leiter bei Stormshield

Die Definition von verdächtigem Verhalten geht über die Kenntnis dieser drei großen Kategorien hinaus und kann sich als recht komplex erweisen. In der Tat muss sich ein Verhalten, das von einer Abteilung oder einem Berufsfeld als verdächtig definiert wird, woanders nicht unbedingt auch als solches herausstellen. „*Heute sind IT-Manager dafür verantwortlich, verdächtiges Verhalten zu definieren. Die IT-Abteilung kann jedoch nicht alles wissen, und bestimmte Berufsfelder weichen mit ihrer Anwendungsweise womöglich weit von der Norm ab und können daher als verdächtig gelten*“, erklärt **Sébastien Viou**, Berater für Cyber-Evangelisten bei Stormshield. Abseits der Funktion einer IT-Abteilung ist es daher sinnvoll, dass jeder Mitarbeiter seine eigenen Anwendungsszenarien definiert und aktiv an der IT-Sicherheit mitwirkt. „Cybersicherheit sollte jeden betreffen“, verdeutlicht Sébastien Viou. **Das Definieren von verdächtigem Verhalten nach Geschäftsbereichen und Anwendungstypen ist ein wichtiger, aber schwieriger Prozess**, da man Anwendungen gleichzeitig kontrollieren und beobachten muss, ohne den Arbeitskomfort einzuschränken.

Verdächtiges Verhalten zu verstehen, zu definieren und schließlich zu erkennen, ist daher keine leichte Aufgabe und erfordert auch eine umfassende Forschung und Analyse. Doch wenn die Aufgabe so anspruchsvoll ist, warum muss man dann definieren, was verdächtiges Verhalten ausmacht? „Das Definieren von verdächtigem Verhalten dient dem Verständnis, was konkret erkannt werden muss. Für Cyber-Akteure ermöglicht diese Übung auch den Wissensaustausch über eine gemeinsame Sprache, insbesondere über die MITRE-ATT&CK-Matrix", informiert **Thierry Franzetti**, technischer Leiter bei Stormshield. Dieser Wissensaustausch ermöglicht es insbesondere, die Techniken zu identifizieren, die für böswillige Zwecke verwendet werden. Diese Analyse erfordert jedoch ein gutes Verständnis der Angriffstechniken und insbesondere der Hauptvektoren von Workstation-Infektionen.

DIE HAUPTVEKTOREN VON WORKSTATION-INFEKTIONEN

Wenn auf einer Workstation verdächtiges Verhalten festgestellt wird, ist normalerweise ein Angriff im Gange oder in Vorbereitung. Es gibt eine Reihe von Infektionsvektoren, die auf diese Workstations abzielen, von denen vier besonders hervorstechen.

Phishing

Der erste Hauptinfektionsvektor ist Phishing, das von 75 bis 80 % der Malware verwendet wird. Phishing ist unter Angreifern beliebt, da es sowohl einfach durchzuführen als auch effektiv ist und sehr viele Personen erreichen kann.

Zum Beispiel entdeckten Kaspersky-Forscher im Dezember 2019, dass Cyberkriminelle die Gelegenheit der Veröffentlichung eines der am meisten erwarteten Filme des Jahres, Star Wars, genutzt hatten, um eine Phishing-Kampagne durchzuführen: Etwa 30 betrügerische Websites, die der des Films ähnelten, wurden entdeckt. Darüber haben die Angreifer viele Internetnutzer in die Irre geführt, indem sie eine kostenlose Version des Films in Aussicht stellten, die vermeintlich von diesen schädlichen Websites heruntergeladen werden konnte. Dank dieser Vorgehensweise konnten die Angreifer die persönlichen Daten der betrogenen Internetnutzer sammeln. Diese Phishing-Angriffe haben in den letzten Monaten vor dem Hintergrund der Corona-Pandemie, die von Angreifern ausgenutzt wurde, ebenfalls erheblich zugenommen. So wurden viele Phishing-Kampagnen zum Thema Gesundheit und Prävention im Zusammenhang mit der COVID-19-Epidemie durchgeführt. Darüber hinaus hat die Verlagerung eines großen Teils der Bevölkerung auf Telearbeit diesen Trend weiter verstärkt. Ersten Zahlen zufolge hätten die Phishing-Versuche beispielsweise in der ersten Woche des Lockdowns um 400 % zugenommen

USB-Geräte

Ein weiterer Vektor zur Infektion einer Workstation sind USB-Geräte wie Mäuse, Sticks

und Tastaturen. Die Masche besteht darin, einen USB-Stick mit böswilligem Inhalt in der Nähe eines Zielunternehmens auf den Boden zu legen. Die natürliche Neugier einiger Mitarbeiter soll dann dafür sorgen, dass der Stick mitgenommen und an eine Workstation angeschlossen wird.

In einer Studie zu Angriffen über USB-Sticks berichtet das Symposium sur la sécurité des technologies de l'information et des communications (SSTIC: Symposium zur Sicherheit der Informations- und Kommunikationstechnologien) über die große Angriffsfläche, die diese Peripheriegeräte und insbesondere die Sticks bieten (Informationslecks, Erhöhung von Berechtigungen usw.) sowie die möglichen Betriebsmodi, die von den Angreifern verwendet werden. Eine Workstation kann beispielsweise infiziert sein, wenn der Benutzer eine der Dateien auf dem Stick öffnet oder der Stick ganz einfach nur an einem Computer angeschlossen ist.

Remote-Desktop-Protokolle

Ein weiterer möglicher Infektionsvektor ist die Kompromittierung von RDPs („*Remote Desktop Protocols*"). Sie ermöglichen den Zugriff auf weiter entfernte Stationen oder Maschinen (Remote Desktops usw.). Dieser Übertragungsweg wird beispielsweise für Ransomware verwendet. Bei der 2015 entdeckten SamSam-Ransomware, die speziell auf Windows-Server abzielt, war das etwa der Fall. Im Jahr 2018 untersuchte das FBI die Vorgehensweise von SamSam und gab bekannt, dass RDP als Infektionsvektor verwendet wird, um Windows-Server anzugreifen.

Auch bei den RDPs verstärkten die Umstände der Pandemie dieses Phänomen und insbesondere Brute-Force-Angriffe. Mitarbeiter greifen durch den Lockdown und die Verbreitung der Telearbeit verstärkt von ihren persönlichen Terminals aus auf ihr berufliches Umfeld zu, ohne unbedingt auf dem aktuellen Stand der IT-Sicherheitsregeln zu sein. Die Anzahl der RDP-Kompromittierungen hat daher erheblich zugenommen.

IT-Sicherheit in der Telearbeit sollte genauso gewährleistet sein wie der Schutz vor anderen Infektionsvektoren, die Cyberangriffsrisiken für Organisationen darstellen. Unternehmen müssen mehr denn je von Cybersicherheits-Fachleuten unterstützt werden, um mögliche Sicherheitsverletzungen zu begrenzen und sogenanntes verdächtiges Verhalten zu überwachen und besser zu verstehen. Dies ist die Basis, um innerhalb des Unternehmens effektiver gegen Cyberkriminalität vorgehen zu können.

ENDPUNKTLÖSUNGEN ALS RETTUNG

Sicherheitslösungen zur Erkennung und Überwachung verdächtigen Verhaltens haben sich weiterentwickelt. Bisher bestand die Lösung zum Schutz vor Cyberangriffen in der Nutzung von Antivirenprogrammen. Ein Ansatz, der sich schnell als unzureichend erwies, da diese Art Software keine oder eine nur unzureichende Verhaltenserkennung besitzt und lediglich mit bekannten Schadcodes umgehen kann. „*Bestimmte*

Angriffstechniken versuchen, sich vor Antivirenprogrammen zu verstecken. Daher müssen Lösungen her, die diese Art der Erkennung ergänzen und auch mit nicht standardmäßigen Anwendungen umzugehen wissen", verdeutlicht Thierry Franzetti. Dann kamen fortschrittlichere Sicherheitslösungen, zunächst mit dem Gebrauch von *„Endpoint Protection Platforms" (EPP), die verdächtiges und eindeutig böswilliges Verhalten erkennen und über Workstation-Schutzfunktionen verfügen. Danach erschien „Endpoint Detection & Response*", die sogenannten EDR-Lösungen. Sie reagieren auf die Anforderung zur Erkennung verdächtigen Verhaltens, da sie sich in einem Prozess der proaktiven Erkennung von noch nicht bekannten Bedrohungen befinden, indem sie alles „abhören", was auf einer Workstation geschieht, und schwache Signale erkennen, etwa den plötzlichen Start zahlreicher Operationen auf derselben Workstation. EPP- und EDR-Lösungen bieten jeweils interessante Schutz- und Erkennungsniveaus und ergänzen sich vor allem je nach Einsatzbereich der Unternehmen. Eine Lösung, die häufig mit EDR einhergeht, ist künstliche Intelligenz (KI). *„Die KI bringt insbesondere eine stärkere Rechenleistung mit sich, die es ermöglicht, unerwartete Verhaltensweisen zu identifizieren und ihnen eine Punktzahl zu geben, um sie dann klassifizieren und besser auf sie reagieren zu können*", erklärt Sébastien Viou. Eine KI, die tatsächlich zunehmend in die Bausteine von Cybersicherheitslösungen integriert wird und über deren Relevanz die Forscher sich einig zu sein scheinen. Beispielsweise hat der britische Geheimdienst kürzlich eine Studie über den Nutzen von KI bei der Bekämpfung von Cyberbedrohungen durchgeführt. Die Identifizierung verdächtigen Verhaltens ist einer der Bereiche, in denen der KI-Einsatz einen echten Mehrwert haben könnte.

Neben Endpoint-Lösungen werden auch andere Verfahren in Betracht gezogen, etwa Sandboxing, mit dem Dateien geöffnet oder unbekannte oder verdächtige Elemente in einer isolierten Testumgebung ausgeführt werden können, ohne das Risiko einer Kompromittierung der Workstation einzugehen.

Zwar gibt es eine Reihe von Sicherheitslösungen, um auf Cybersicherheitsprobleme in Unternehmen und insbesondere auf Probleme im Zusammenhang mit verdächtigem Verhalten zu reagieren, doch müssen selbige unter Berücksichtigung der Kontexte implementiert werden, für die sie gelten. Die Rolle der Entwickler besteht darin, im Voraus das verdächtige Verhalten klar zu definieren. *„Eine Sicherheitslösung ist nur ein Werkzeug. Entscheidend ist die Art und Weise, wie sie konfiguriert und gewartet wird*", verdeutlicht Sébastien Viou. Entwickler müssen daher in der Lage sein, ihre Lösungen vorab zu konfigurieren, indem sie alle Maßnahmen und Regeln (konfigurierbare Regeln,

die sich an jeden Kontext oder jedes Unternehmen anpassen) einbetten, damit die richtige Erkennungsstufe bereitgestellt werden kann. Aber auch, um Administratoren eine einfach einzurichtende Umgebung bereitzustellen. Um effektiv zu sein, müssen Lösungen daher Schutzmaßnahmen (Verwaltung von Geräten, Erhöhung von Berechtigungen usw.) und zugehörige Verhaltensmuster kombinieren. Darüber hinaus sind Endpoint-Lösungen nicht unfehlbar, und es kommt zu Fehlalarmen. „*Obwohl es uns gelingt, grundlegende Schutzelemente zu definieren, ist die Vielfalt verdächtiger und nicht verdächtiger Verhaltensweisen auf einer Workstation so groß, dass es immer Ausnahmen geben wird*“, analysiert Thierry Franzetti. Um Fehlalarme zu begrenzen, ist es ideal, eine Whitelist (oder Allowlist) definieren zu können, um legitime Anwendungen nicht zu blockieren. Um vollständig wirksam zu sein, ist es interessant, diesen Ansatz für jedes Unternehmen maßzuschneidern und damit den Schutz an unterschiedliche Verhaltensweisen anzupassen.

Ein Fenster in Ihrem Internetbrowser anzeigen, ein Word- oder PDF-Dokument öffnen oder Dateien herunterladen: Alltägliche Geschäftsabläufe wie diese werden die IT-Sicherheitsabteilungen zweifellos noch einige Zeit beschäftigen. Und verdächtiges Verhalten, ein Hauptthema der Cybersicherheit in Unternehmen, macht es uns weiterhin nicht leicht.