STORMSHIELD

MEINUNGEN

CYBERSICHERHEIT: WENN KNOW-HOW VON GESTERN UND TECHNOLOGIEN VON MORGEN HAND IN HAND GEHEN

Julien Paffumi
Product Management Leader, Stormshield

„*In alten Töpfen kocht es sich am besten*“. So lautet eine französische Volksweisheit, die auch auf die Cyberwelt Anwendung finden könnte. Denn hier werden Technologien der Zukunft und neue Gebrauche unter einen Hut gebracht, wobei man sich gleichzeitig auf sein Know-how stützt und altbewährte Methoden auf den aktuellsten Stand bringt. Wir haben einige Überlegungen angestellt.

Bis wohin wird uns die Innovation in der Cyberwelt bringen? Diese Frage ist heute in aller Munde, es gibt hierauf jedoch keine Antwort. Und insbesondere darf hierbei auch nicht die Bedeutung der gemeinsamen Kenntnisse vergessen werden. Denn die Innovation ist zwar einer der Grundpfeiler dieses Bereichs, **in der Cyberwelt ist jedoch auch der Gebrauch eines soliden Know-hows und die Wiederverwendung alter Methoden tief verankert**.

Märkte, die bislang nicht von Cyber-Bedrohungen betroffen waren, befinden sich nun mitten im Gefecht und der nächste Cyberangriff in den Medien wird wahrscheinlich größtenteils auf den Grundsteinen eines vergangenen Angriffs aufbauen. Eine kunstvolle Mischung zwischen Altem und Neuem also, die sowohl den Interessen der Großunternehmen der Cybersicherheit als auch jenen der Angreifer dient. Dies führt dazu, dass das Ökosystem einem nahezu stetigen Wettlauf zwischen den beiden Lagern unterliegt. Aus diesem Grund liegt es im Interesse der Verteidiger, ihre Kenntnisse zusammenzulegen und bewährte Sicherheitsverfahren auszutauschen.

KNOW-HOW: FÜR GEWISSE BRANCHEN VERALTET, FÜR ANDERE WIEDERUM PERFEKT

Wenn man an die Cybersicherheit denkt, geht der Gedanke sofort in Richtung „IT" (Informationstechnologie), wozu alles zählt, was mit Informatik und Internet in Berührung kommt. Man denkt weniger oft an „OT" (für *„Operational Technology"*), die besonders in der Industrie Anwendung findet. Diese Branche öffnet sich immer mehr und ist einer vollumfänglichen Umgestaltung unterworfen, weshalb Probleme in Verbindung mit der Cybersicherheit auftreten.

Die IT entwickelt sich stetig weiter: neue Anwendungen, neue Geräte, neue Gebrauche oder sogar neue Zielgruppen, da die Senioren sich nun auch hiermit befassen. Die Cybersicherheitsunternehmen haben sich damit abgefunden, mit dieser ungezügelten Weiterentwicklung zu leben und sich neue Schutzmechanismen auszudenken, ohne für alles eine Antwort haben zu können. *„Man muss das Risiko akzeptieren und sich auf dieser Grundlage Sicherheitslösungen ausdenken"*, so **Matthieu Bonenfant,** Marketingleiter bei Stormshield. Demgegenüber wird die OT weitaus stärker kontrolliert und im Voraus definiert. Jeder Befehl jeder Komponente des Industriesystems ist von Bedeutung und muss bekannt und erfasst sein. Dies ist genau das Gegenteil einer Improvisation, da es hier um viel geht: *„Wenn man das Risiko eingeht, beispielsweise bei einer Transformatorstation einen falschen Befehl einzugeben, dann geht man das Risiko ein, das ganze Netzwerk lahmzulegen"*, fügt Matthieu Bonenfant hinzu.

Wo liegt jetzt nun die Gemeinsamkeit zwischen IT und OT? Es ist die Cybersicherheit und genauer gesagt die Fähigkeit der Cyberwelt, gewisse bewährte Verteidigungsmethoden neu zu verwenden. Schutzmethoden, die bereits Jahrzehnte lang in der IT effizient genutzt werden, können auch genauso gut in der OT eingesetzt werden. Denn die OT wird seit dem Aufkommen der Industrie 4.0 hart von den Cyberproblemen getroffen. *„Die Cybersicherheit in der Industrie steckt noch in den Kinderschuhen. Was vor einigen Jahren für die IT funktionierte kann allerdings heute auch für die OT funktionieren"*, erklärt **Adrien Brochot,** Product Manager bei Stormshield. Hiervon ausgehend müssen die Cybersicherheitsunternehmen – und somit die Entwickler – in der Lage sein, dies zu nutzen und ihr Know-how auszutauschen, damit bestehende Verteidigungsarten auf diese neuen Infrastrukturen angepasst werden können.

Dies ist beispielsweise der Fall des IPS (*Intrusion Prevention System*), mit dem man eine ausführliche Analyse der Netzwerkkommunikationen vornehmen kann, um zu prüfen, ob die Schwachstelle eines Protokolls ausgenutzt wird oder ein unrechtmäßiger Befehl eingefügt wurde. Das IPS wird in der IT weiterhin gebraucht, es ist für die Industrie aber noch unentbehrlicher, da dort die Folgen der Änderung des Inhalts der Verbindungen fatal sein können. Vor diesem Hintergrund ist es oftmals von kritischer Bedeutung, dass nur rechtmäßige und erfasste Verhaltensweisen autorisiert werden. Die OT war bislang nur zu einem sehr niedrigen Grad mit dem Internet verbunden. Heutzutage werden die operativen Netzwerke jedoch direkt oder indirekt mit dem Internet verbunden sowie auch die Produktionslinien. Aus diesem Grund sind sie Cyberbedrohungen und Angriffen ausgesetzt, die in der Vergangenheit gegen die IT eingesetzt wurden.

AUS ALT WIRD NEU: DIE CYBERANGRIFFE KOMMEN NICHT ZU KURZ

Die Angriffe kommen allerdings nicht zu kurz, da auch ihnen die zahlreichen möglichen Weiterentwicklungen der Cyberwelt zugutekommen: Ihnen kommen sowohl das Know-how von gestern als auch die technologischen Fortschritte zugute.

„In Wirklichkeit beruhen 90 % der neuen Angriffe auf alten Angriffen und die Angreifer passen diese lediglich an, um die Sicherheitsschwellen zu übersteigen und in ein System einzudringen"

Adrien Brochot, Product Manager Stormshield

Die Angreifer machen sich zwar neue Schwachstellen und Umgebungen zunutze, die Prinzipien der Ausnutzung dieser Schwachstellen und Umgebungen kommt jedoch nur schwerfällig voran. Und um die Cyberangriffe auch rentabel zu gestalten, greifen die Cyberkriminellen oftmals auf Methoden zurück, die sich bereits bewährt haben. *„In Wirklichkeit beruhen 90 % der neuen Angriffe auf alten Angriffen und die Angreifer passen diese lediglich an, um die Sicherheitsschwellen zu übersteigen und in ein System einzudringen*", erklärt Adrien Brochot. Denn die Wiederverwendung steht bei der Cybersicherheit hoch im Kurs. Gewisse „neue" Malwares sind nämlich in Wirklichkeit nur Abwandlungen ihrer Vorgänger.

Aus diesem Grund werden die Datenbanken, die diese Malwares und ihre zahlreichen Abwandlungen erfassen, zu umfassend und schwer, um von den Betriebssystemen unterstützt zu werden. Diese Datenbanken erfassen deshalb nur die neusten Malwares, weshalb die Angreifer alte Malwares nutzen können, die beinahe in Vergessenheit geraten sind ... Nehmen wir das Beispiel der Malware Emotet, deren erste Angriffe laut der Agence française nationale de la sécurité des systèmes d'information (ANSSI) im Jahr 2014 zu beobachten waren und die diesen Herbstanfang 2020 wieder aktiv wird.

Die Cyberangriffe finden auch häufig zu unterschiedlichen Zeitpunkten statt. Dies ist einerseits darauf zurückzuführen, dass sie sich in der Vergangenheit bereits bewährt haben und andererseits, weil auch, wenn es Patches gibt, nachdem eine Schwachstelle entdeckt wird, nicht alle diese Patches installieren, zumindest nicht gleichzeitig: Diese Zeitspanne stellt dann den perfekten Eintrittspunkt für die Angreifer dar, die sich diese neu entdeckte Schwachstelle ebenfalls zunutze machen.

Denn seit mittlerweile einigen Jahren werden die Entdeckungen von Schwachstellen und die Cyberangriffe in den Medien in den Vordergrund gerückt und fallen je nach Modeerscheinung unterschiedlich aus. Somit dienen sie zugleich den Interessen jener, die sich hiervor schützen möchten, wie auch jener, die diese ausnutzen möchten. Gewisse Angriffstypen finden in den Medien großen Anklang, wie beispielsweise die Ransomwares, die Erpressungen per Webcam oder die berühmten Chef-Betruge. Diese Art der Angriffe war in den vergangenen Wochen mit der Covid-19-Krise besonders groß im Kommen: Es ist eine steigende Anzahl an Identitätsdiebstahlen (Minister, Krankenhausleiter und andere wichtige Personen der Gesundheitskrise) zu beobachten, mit dem Ziel, Geld zu erschleichen. Es gibt jedoch auch Arten von Angriffen, die ganz im Gegenteil nicht in den Medien hervorgehoben und von einem Teil des Ökosystems, der diese analysiert, im Hinterkopf behalten wird. Hierbei handelt es sich um beispielsweise staatliche Behörden, die diese Methode nutzen, um die Schwachstellen dann ganz heimlich auszunutzen. Wenn man sich mit dem Thema ausführlicher befassen möchte, ist die Folge „*Shadow Brokers*“ des Podcasts **Darknet Diaries** ein Muss.

„Für die Angreifer ist es stets wichtig, sich schlecht geschützte Bereiche zunutze zu machen"

Matthieu Bonenfant, Marketingleiter bei Stormshield

„Die Weiterentwicklung der Cyberangriffe ist in etwa so wie die Weiterentwicklung der Mode: es gibt neue Sachen, alte Sachen und neue Sachen, die ihren Ursprung in alten Sachen haben“, lacht Matthieu Bonenfant, der fortführt: *„Gewisse alte Methoden werden schnell an ihre Grenzen stoßen und deshalb angepasst und aktualisiert werden, um leistungsfähiger zu werden. Dies geht dann immer so weiter*“. Im Jahr 2017 wurde über die Ransomware Wannacry viel Tinte vergossen, da sie einige große Unternehmen und Organisationen teilweise lahmlegte. Dabei wies die Verbreitungsart von Wannacry, ebenso wie NotPetya einige Monate später, zahlreiche Ähnlichkeiten zu dem Wurm Conficker von 10 Jahren zuvor auf.

Nutzung alter Sachen, Anpassung der Cyberangriffe, Ausnutzung der technologischen Fortschritte usw. Wenn man die Weiterentwicklung der Cyberangriffe in einer einzigen Idee zusammenfassen müsste, hat Matthieu Bonenfant einen Vorschlag: *„Für die Angreifer ist es stets wichtig, sich schlecht geschützte Bereiche zunutze zu machen*“.

WIE STEHT ES MIT ABER MIT DEN CYBERSICHERHEITSLÖSUNGEN?

Denn die Schlüsselrolle der Cybersicherheitslösungen ist doch der Schutz. Zum Schutz muss man jedoch zunächst bestimmen, wie Cyberangriffe funktionieren, und Cybervorfälle verstehen. Die Vorgehensweisen der Angreifer analysieren und die jüngst entdeckten Schwachstellen stets überwachen, Systeme einrichten, welche die „Spuren" der Cyberangriffe erfassen können: All dies sind Schlüsselelemente, die eine angemessene Verteidigungslinie ermöglichen.

Die Sicherheitsanalysten spielen bei der Handhabung eines Cyberangriffs eine wichtige Rolle. Sie müssen sowohl den Angriffsvektor (das Netzwerk, ein USB-Stick usw.) identifizieren als auch die Einzelheiten des Angriffs verstehen sowie seine Verbreitung innerhalb der Netzwerke, ob nun IT- oder operative Netzwerke. Diese Kenntnis ist erforderlich, um das Cyber-Ökosystem gut beherrschen zu können – die verschiedenen Arten von Angriffen auflisten, über einen Schwachstellen- oder Patchkatalog verfügen –, jedoch auch, um Abstand gewinnen zu können und die Cybersicherheitslösungen entsprechend anzupassen. Der technische Gesichtspunkt ist also von wesentlicher Bedeutung, um einen Cyberangriff zu analysieren und seine Auswirkungen zu verstehen.

Die Entwicklungskurve der Cyberwelt ist eine Herausforderung für die Cybersicherheitsunternehmen und insbesondere die Entwickler, die sich einerseits auf neue Methoden und ihre Weiterentwicklung konzentrieren müssen, andererseits aber die Gegenwart der Cyberwelt nicht aus den Augen verlieren dürfen. Auf gewisse Weise haben sie die Aufgabe eines Gedächtnisses. Sie dürfen alte Schutzmethoden, die mit der Zeit weniger verwendet werden, nicht links liegen lassen, da die Angreifer genau darauf warten. Ebenso wie die Malware Emotet, die zuvor in diesem Artikel angesprochen wurde, kommen auch andere Malwares regelmäßig mit verheerenden Auswirkungen zurück auf die Bildfläche. Hierzu zählen beispielsweise jene, die Macros in der Office-Suite verwendeten. Eine Malware ist genau dann am gefährlichsten, wenn man sie als verschollen ansieht.

Im Rahmen der Kontinuität zwischen Altem und Neuem spielen die Entwickler von Cybersicherheitslösungen „*eine kritische Rolle des Informationsgebers innerhalb des Ökosystems: Konferenzen, Messen, Verfassung von White Books, Präsentation von Use Cases usw.*", erklärt Adrien Brochot. Seiner Meinung nach erleichtern dieser Austausch und diese Tools die Weitergabe von Kenntnissen und die Nutzung innerhalb der Cyber-Community.

DIE BEDEUTUNG DER WEITERGABE VON KENNTNISSEN UND BEWÄHRTEN VERFAHREN

Um die Weiterentwicklung der Cyberwelt und der digitalen Ära bestmöglich zu nutzen, ist es im Sinner aller Akteure der Cybersicherheit, sich als ein einziges Ökosystem und die Cybersicherheit als gemeinsames Ziel und gemeinsame Verantwortung zu sehen. Viele der Akteure dieses Ökosystems sind zwar Konkurrenten, dies hält sie jedoch

nicht davon ab, Informationen und Kenntnisse untereinander auszutauschen und Partnerschaften zu schließen. Ferner bestehen zahlreiche technische Datenbanken, die von der Community gespeist werden, wie VirusTotal, die verdächtige Dateien, die potenziell Malware enthalten, analysiert und erfasst, oder MITRE ATT&CK, die zahlreiche Angriffsmethoden erfasst und es den Cyberunternehmen ermöglicht, auf ein aktuelles Bezugssystem zuzugreifen.

Diese Weitergabe von Kenntnissen kann auch mittels öffentlichen Interessengruppen geschehen, wie das Portal cybermalveillance.gouv.fr, auf dem Unternehmen und Privatpersonen im Internet verübte böswillige Aktivitäten melden können. Eine weitere Möglichkeit sind die Melde- und Reaktionszentren für IT-Angriffe (die berühmten CERT, für Computer Emergency Response Team, oder die CSIRT, für Computer Security Incident Response Team), die in Echtzeit über die wichtigsten Cyberbedrohungen informieren. Diese CERT können öffentlich oder privat, national (CERT-FR für Frankreich) wie auch international (CERT-EU für das europäische Äquivalent) sein. *„Das Cyber-Ökosystem umfasst zahlreiche Informationen und Tools, die Kenntnisse werden jedoch auch sehr unterschiedlich präsentiert und erfasst: Die erfolgreiche Auslese und der schnelle und einfache Zugriff auf Informationen im Bedarfsfall stellen also eine gewisse Herausforderung dar*“, so Matthieu Bonenfant.

Die technische Komponente (aka die Sicherheitsanalysten) spielen auch hier eine wichtige Rolle, da sie es dem Ökosystem ermöglichen, seine bewährten Sicherheitsverfahren und sein Know-how weiterzugeben. Diese Experten verfügen über ihr eigenes Ökosystem in der Cyber-Community, abgeschieden von eventuellen geschäftlichen Fehden oder sonstigen Wettbewerbsstrategien. Und dies stellt für die Cyberunternehmen einen wirklichen Vorteil und Mehrwert dar, da die Zusammenlegung der Kenntnisse hier vor allem unter technischen Aspekten geschieht. Und das Ökosystem profitiert von dem Willen, Neues zu lernen. Somit analysieren und teilen die technischen Analysten ihre Funde mit dem Ziel der stetigen Verbesserung.

Die Weitergabe von Kenntnissen und bewährten Cybersicherheitsverfahren stellt also eine wesentliche Komponente des Ökosystems dar, da sie die Cyberunternehmen anhält, über sich hinauszuwachsen, sich zu verbessern, sich weiterzuentwickeln und Lösungen der Zukunft zu erdenken, die immer leistungsfähiger sind. All dies im Dienste der Prävention und der Analyse der Risiken.

STORMSHIELD

Weltweit müssen Unternehmen, Regierungsinstitutionen und Verteidigungsbehörden die Cybersicherheit ihrer kritischen Infrastrukturen, sensiblen Daten und Betriebsumgebungen gewährleisten. Die auf höchster europäischer Ebene zertifizierten Stormshield-Technologien sind die richtige Antwort auf IT- und OT-Risiken und erlauben den Schutz der Geschäftstätigkeit. Unsere Mission: Cybersorglosigkeit für unsere Kunden, damit diese sich auf ihre Kerntätigkeiten konzentrieren können, die für das reibungslose Funktionieren von Institutionen, Wirtschaft und Dienstleistungen für die Bevölkerung so wichtig sind. Die Entscheidung für Stormshield ist eine Entscheidung für eine vertrauenswürdige Cybersicherheit in Europa. Weitere Informationen finden Sie unter www.stormshield.com.