STORMSHIELD

MEINUNGEN

WARUM STELLEN UPDATES EIN PROBLEM IM BEREICH DER CYBERSICHERHEIT DAR?

Adrien Brochot
Product Manager,
Stormshield,

Ach ja, Updates ... Die berühmten Updates, die mit dem Etikett „verpflichtend“ versehen sind. Eigentlich sind Updates gut gemeint. Auch wenn es oft schwierig ist, die richtige Entscheidung hinsichtlich Computersicherheit auf Kosten der Produktion zu treffen, kann das Thema Updates nicht mehr weiter ignoriert werden. Im Gegenteil, es muss zu einem zentralen Thema der Sicherheitspolitik von Unternehmen werden.

Warum sollte man Updates vornehmen? **Sind Updates wirklich unbedingt notwendig?** Kann das nicht noch etwas länger warten? Diese Fragen - und viele andere - stellen sich noch immer allzu oft in vielen Unternehmen, die digitale Hygiene, IT-Schutz und gute Sicherheitspraktiken nicht mit Updates in Verbindung bringen und diese auch nicht allzu wichtig nehmen. Für sie stehen Geschäftskontinuität und Produktionskapazität nach wie vor im Vordergrund und die Behebung von IT-Schwachstellen wird oft nebensächlich.

So wie die geschäftliche Produktion nicht unterbrochen werden darf, werden auch die Cyber-Angriffe nicht aufhören... Solange es Schlupflöcher gibt, wird es Angriffe geben. Und genau dafür sind Updates notwendig: um diese Schwachstellen zu beseitigen und die Angriffe abzuwehren! Obwohl es nicht mehr darum geht, ihre Wirksamkeit und Bedeutung nachzuweisen, so muss noch einiges an Überzeugungsarbeit geleistet werden. Die Unternehmen sehen sich vor zwei Herausforderungen, die sie gleichzeitig bewältigen müssen: einerseits die betrieblichen Anforderungen und andererseits der Kampf gegen die Cyberrisiken, die ihre Tätigkeiten bedrohen.

VERNACHLÄSSIGTE UPDATES UND ANFÄLLIGE SYSTEME

Die hier behandelten Fehler und Schwachstellen, die von den Akteuren für Cybersicherheit dokumentiert und veröffentlicht werden, können von kleinen Bugs bis hin zu kritischen Sicherheitslücken reichen. Obwohl diese Informationen für Unternehmen bestimmt sind, profitieren Angreifer ebenfalls davon. Systeme, die nicht aktualisiert werden, sind daher besonders anfällig für Cyber-Angriffe. *„Angreifer richten Fingerabdrucksysteme ein - Scans von Netzwerken und Umgebungen zur Identifizierung von Rechnern -, um schnell und einfach angreifbare Computer zu erkennen, in diesem Fall solche, die nicht aktualisiert werden*“, sagt **Guillaume Boisseau** von der Abteilung Professional Services von Stormshield. Es ist unbestreitbar, dass **nicht aktualisierte Systeme den Angreifern die Gelegenheit bieten, böswillige Handlungen durchzuführen.** *„Angreifer werden ihren Angriff je nach Informationssystem vorantreiben, insbesondere wenn es sich um alte Systeme mit bekannten und bereits vom Netzwerk der Cyberangreifer genutzten Sicherheitslücken handelt*“, fügt **Maxime Nempont**, Technischer Leiter Security bei Stormshield, hinzu.

Wenn es um nicht aktualisierte Arbeitsplätze geht, ist Ransomware WannaCry ein perfektes Beispiel für die Anfälligkeit von Arbeitsplätzen. Im Mai 2017 hatte sich die Ransomware dank einer Sicherheitslücke in den Windows-Umgebungen in Systemen verbreitet, in denen die Sicherheitslücke nicht geschlossen wurde. Microsoft hatte zwei Monate vor dem Angriff den Sicherheitspatch für diese Schwachstelle veröffentlicht und vor deren Kritikalität gewarnt. Das Resultat: 150 Länder wurden durch den WannaCry-Cyberangriff lahmgelegt, und die finanziellen Verluste betragen heute Milliarden Dollar.

WannaCry ist ein Abbild der Realität, die man heute noch kennt: Viele Unternehmen sind sich noch immer nicht bewusst, was es bedeutet, Updates zu machen und diese in kürzester Zeit vorzunehmen, um die Angriffsfläche zu verkleinern.

„Updates sind ein wenig wie Zahnarztbesuche: Wenn man regelmäßig zur Kontrolle geht, gibt es jedes Mal nur kleine Dinge zu behandeln. Wenn man aber zu lange darauf wartet, sich einer Behandlung zu unterziehen, wird es immer schlimmer.“

Guillaume Boisseau, Abteilung Professional Services von Stormshield

Im Mai 2019 veröffentlichte Microsoft eine Sicherheitslücke, diesmal in einer seiner Systemkomponenten. Dieser als „BlueKeep" bezeichnete Bug hätte die gleiche Größenordnung wie WannaCry erreichen können, wenn er in großem Maßstab ausgenutzt worden wäre. Obwohl die Forscher für Cybersicherheit noch nicht sagen können, dass BlueKeep in großem Maßstab von Angreifern ausgenutzt wurde, so war das Risiko reell vorhanden. Denn einen Monat nach Aufdeckung des Fehlers und der Veröffentlichung des Patch von Microsoft waren immer noch fast eine Million Systeme ungeschützt und anfällig. Also ebenso viele Möglichkeiten für bösartige Ökosysteme, um dort einzudringen ...

„Einige Unternehmen führen ihre Updates nicht durch, weil es ihnen an Verfahren fehlt, die einen Rahmen dafür bieten (wie z. B. fehlende Testumgebungen), und die Updates sammeln sich an, und das Risiko steigt. Das kann man mit einem Zahnarztbesuch vergleichen: Wenn man regelmäßig zur Kontrolle geht, gibt es jedes Mal nur kleine Dinge zu behandeln. Wenn man aber zu lange darauf wartet, sich einer Behandlung zu unterziehen, wird es immer schlimmer. Das Gleiche gilt für Updates!" sagt Guillaume Boisseau.

Die Bedrohung von WannaCry scheint sich regelmäßig zu wiederholen: Dieses Jahr wurde unter dem Namen SMBGhost ein weiterer wichtiger Bug im Zusammenhang mit dem Windows-Betriebssystem entdeckt. Eine Schwachstelle, die sich auf demselben Protokoll befand, wie jenes, auf das WannaCry abzielte. Wäre diese Lücke ausgenutzt worden, wären die Folgen katastrophal gewesen.

Angriffe, die auf nicht aktualisierte Systeme abzielen, nehmen zu, und dies wird nicht aufhören; sie sind einfach durchzuführen und gut dokumentiert und stellen somit einen Anreiz für die Angreifer dar, auf den sie nicht verzichten. **Mehr denn je muss daher die Implementierung von Updates von allen Unternehmen** – unabhängig von der Branche – als Priorität betrachtet und zu einem integralen Bestandteil der Unternehmenskultur werden.

CYBERSICHERHEIT UND BETRIEBLICHE ANFORDERUNGEN IN EINKLANG BRINGEN: SEIT JEHER ANGESTREBT, ABER NIE ERREICHT

Aktualisierungen von Software, Anwendungen oder Geräten waren schon immer problematisch: einerseits das Ziel, die Sicherheit zu gewährleisten und andererseits die operativen Anforderungen zu berücksichtigen, die jede Tätigkeit mit sich bringt.

Auch wenn Updates dazu da sind, Bugs zu beheben und kritische Schwachstellen mit Patches zu schließen, tragen sie auch ihren Teil zu Einschränkungen in Unternehmen bei. In der Industrie und in der Betriebstechnologie (OT) sind Updates besonders gefürchtet, da sie zu unerwünschten Effekten wie einen längeren Produktionsstillstand führen können. Auch nach Abschluss der Updates muss die Systemwiederherstellung in der Industrie genau beobachtet werden. Aufgrund des Rebound-Effekts können

unvorhergesehene Folgen zu einem Produktionsrückgang führen, was sich wiederum auf den Absatz auswirkt. „*Die Beurteilung der Notwendigkeit einer Aktualisierung durch eine Risikoanalyse und die Planung des Updates durch Messung der Auswirkungen auf die Produktion sind daher obligatorische Aspekte, die in der Industrie berücksichtigt werden müssen*“, betont **Florian Bonnet**, Leiter des Produktmanagements bei Stormshield. „*Deshalb müssen Wartungszyklen in der Industrie richtig vorbereitet und geplant werden.*“

Aber die Einschränkungen betreffen nicht nur die OT-Netzwerke. Updates können ganz allgemein Rückschritte verursachen und dazu führen, dass eine Website nicht mehr verfügbar ist oder den Benutzer Zeit kostet, weil er gezwungen ist, seine Geräte neu zu starten und deshalb Bürotätigkeiten für eine Weile einzustellen muss. Dieselben Updates können auch wegen der darin eingebetteten Komponenten restriktiv sein und sich direkt auf die in Entwicklung befindliche Software oder Anwendungen auswirken - sehr zum Leidwesen der Entwickler! – Oder auch auf die bereits implementierten Anwendungen eines Arbeitsplatzes.

Unabhängig davon, ob Sie Leiter eines Textilproduktionsbetriebs, Webentwickler oder eine ganz normale Person an ihrem Schreibtisch sind, werden Updates häufig nur widerwillig durchgeführt und lösen Bedenken und Ablehnung hinsichtlich ihrer Durchführung aus. Die Frage der Updates ist also ebenso komplex wie paradox.

DIE FRAGE DER AUSWIRKUNG VON UPDATES

Sollte man also Updates vornehmen oder nicht? Aktualisieren oder nicht aktualisieren? Das ist die Frage! Und last but not least: Je nach betrieblichen Zwängen und Arbeitsumgebungen (Produktionsumgebungen, verwendete Anwendungen usw.) können Updates sehr komplex, wenn nicht gar unmöglich sein. „*Vor einer Aktualisierung ist viel Arbeit zu leisten, um in der Lage zu sein festzulegen, ob sie sich auf den Arbeitsplatz oder die Arbeitsumgebung auswirken kann. Bei sensiblen Umgebungen und kritischen Systemen ist es zum Beispiel notwendig, eine Vorproduktion in Betracht zu ziehen, für den Fall, dass die Aktualisierung zu einer Fehlfunktion des Systems - oder einer Änderung seiner Funktionsweise – führt*“, erklärt Guillaume Boisseau.

Man muss also von der Annahme ausgehen, dass in der wunderbaren Welt der Updates Kontrollverfahren und vorausschauendes Handeln die Schlüsselwörter sind. Dasselbe gilt auch bei automatisierten Updates (PC, Tablets usw.), bei denen es ebenfalls notwendig ist, die Zuverlässigkeit zu überprüfen, um die Risiken eingrenzen zu können. „*In der IT können automatische Updates für Arbeitsplätze oder die Bürotechnik aktiviert werden, da es möglich ist, sie zu verzögern und auf einen passenden Zeitpunkt zu verlegen*“, erklärt Florian Bonnet. Er meint abschließend, dass „*es auf Ebene der IT-Server oder in den OT andererseits nicht möglich ist, Updates zu automatisieren, da wir uns in kritischeren Systemen befinden, bei denen die Folgen von Updates perfekt unter Kontrolle gehalten werden müssen.*“

In einigen Fällen sind Updates tatsächlich nicht ohne weiteres durchführbar und erfordern den Einsatz von hochverfügbaren Architekturen – oder sogar von digitalen Zwillingen oder anderen Virtualisierungsplattformen –, um sie zu testen. In Betriebsnetzwerken ist diese Testumgebung daher unerlässlich, um die Risiken einer Aktualisierung zu bewerten und eine Unterbrechung des Betriebssystems zu vermeiden.

Andere Gegebenheiten machen Updates unmöglich, z. B. „*wenn ein Update dazu führt, dass die Anwendung mit einem älteren Betriebssystem nicht kompatibel ist, oder wenn es sich um ein End-of-Life-System handelt, bei dem die Aktualisierung und Migration auf ein neues System zu kostspielig wird*", führt Maxime Nempont weiter aus. Vor diesem Hintergrund ist es nicht schwer sich vorzustellen, dass Unternehmen trotz der Herausforderungen im Bereich der IT-Sicherheit zuerst zögern werden, ein Update durchzuführen, als sich sofort dafür zu entscheiden. Die Verleger spielen daher eine Schlüsselrolle, sowohl als Berater als auch als Vermittler, um die Unternehmen bei der Durchführung ihrer Updates zu unterstützen und Alternativen vorzuschlagen, wenn diese undurchführbar sind. Ihr Ziel? **Die Entwicklung möglichst einfacher Systeme für Updates und sicherstellen**, dass die Unternehmen davon profitieren können.

Es sind jedoch in erster Linie die Unternehmen selbst, die Bedeutung der Updates und ihre Anwendbarkeit bewerten müssen. **Denn wer diese Updates nicht durchführt, setzt sich Cyber-Angriffen aus**, für die verwundbare Systeme ein begehrtes Einfallstor sind.

SICH DIE „KULTUR FÜR UPDATES" ANEIGNEN

Obwohl Unternehmen im Allgemeinen immer sensibler auf die Frage von Updates reagieren, können sie dennoch Schwierigkeiten haben, die Risiken einzuschätzen oder zu verstehen, die sie eingehen, wenn sie ein Update nicht durchführen. Darüber hinaus sind sich nicht alle Unternehmen bewusst, dass sie das Ziel eines Cyberangriffs sein könnten. Das ist im Betriebsnetzwerk der Fall, wo die Cyberkultur noch nicht stark genug entwickelt ist. Doch, wie Florian Bonnet daran erinnert „*ist die Frage nicht mehr, ob man angegriffen wird, sondern wann*" und fügt hinzu: „*Die Annahme der Kultur für Updates erfolgt auch über eine Akzeptanz des Cyber-Ökosystems im Allgemeinen, indem man die Nachrichten verfolgt, die Dinge im Auge behält…*". Es gibt also ein Bewusstsein, das entwickelt werden muss, und die Herausgeber sind da, um das zu fördern.

Beweise durch Aufführen von Beispielen ist eine Methode, die laut Maxime Nempont recht gut funktioniert, für die „*es notwendig ist, konkrete Fälle herzunehmen, über reale Ausnutzung kritischer Sicherheitslücken zu sprechen und verständlich zu machen, dass all dies nicht nur theoretisch ist*". Neben der Sensibilisierung müssen die Herausgeber den Updatevorgang auch begleiten und präzise sein, wenn sie dem Kunden eine neue korrigierte Version bereitstellen: Es muss klar erkennbar sein, ob es sich um die Behebung eines Bugs oder einen Patch für eine Sicherheitslücke handelt. „*Der Herausgeber muss eine Art Rechtfertigung für die von ihm angebotenen Updates geben und eine gute Darstellung der damit verbundenen Risiken präsentieren, um ein Unternehmen zu beruhigen. Denn auf die eine oder andere Weise werden die Kunden immer versucht sein, der Produktion den Vorrang vor allem anderen zu geben*", ist sich Guillaume Boisseau bewusst.

„Die Frage ist nicht mehr, ob man angegriffen wird, sondern wann."

Die erzieherische Aufgabe der Herausgeber steht daher im Mittelpunkt des Prozesses der Akzeptanz durch Unternehmen, aber nicht nur. Auch IT-Manager spielen in diesem Prozess eine wesentliche Rolle. Die Updates und die damit verbundenen Verfahren (Häufigkeit der Updates, Aktivierung von automatischen oder nicht automatischen Updates usw.) liegen in der Tat in der Verantwortung der IT-Abteilungen und müssen auf ihrer Ebene und nicht auf der Ebene der Benutzer gesteuert und zusammengeführt werden. Die IT-Teams sind am besten in der Lage, korrekt auf das Problem der Updates zu reagieren und die richtigen Mittel für die Überwachung für deren Durchführung bereitzustellen.

Doch einige Länder, wie die Vereinigten Staaten, haben auf Pädagogik gestütztes Handeln gegen stärkere Zwangsmaßnahmen getauscht, die angesichts der jüngsten Bedrohung durch Zerologon - einer Sicherheitslücke, die Windows-Server in Unternehmensnetzwerken betrifft - eine entschlossene Haltung eingenommen haben. Sollte dieses Schlupfloch ausgenutzt werden, könnte ein Angreifer die Kontrolle über anfällige Rechner, einschließlich Domänencontroller, übernehmen. In diesem Zusammenhang hat das amerikanische Ministerium für Innere Sicherheit einen harten Schiedsspruch erlassen: Alle Regierungsbehörden des Landes mussten die Aktualisierung zur Behebung dieser Schwachstelle bis zum 21. September um Mitternacht mit entsprechenden Nachweisen umgesetzt haben. Um diesen Punkt nicht zu erreichen und den erzieherischen Prozess so gut wie möglich zu unterstützen, ist es am besten, sich auf die Anpassung der Unternehmen zu konzentrieren, sie in ihren Bemühungen zum Verständnis zu unterstützen, und ihnen die Gewissheit zu geben, weiter produktiv bleiben zu können und gleichzeitig ein korrektes Sicherheitsverhalten zu haben.

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.