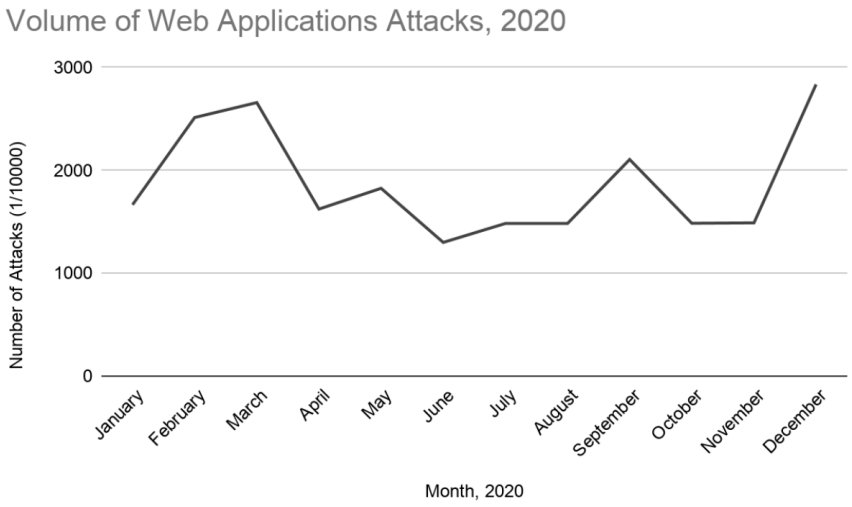
Angriffe von Webanwendungen auf das Gesundheitswesen steigen um 51%, da COVID-19-Impfstoffe eingeführt werden

Als im Dezember die ersten COVID-19-Impfstoffe verbreitetet wurden, überwachten die Imperva Research Labs einen erstaunlichen Anstieg der Angriffe von Webanwendungen auf Ziele im Gesundheitswesen um 51%. Die Aktivität schließt ein beispielloses Jahr der Cybersicherheitsaktivitäten ab. Imperva-Daten zeigen, dass die Gesundheitsbranche weltweit durchschnittlich 187 Millionen Angriffe pro Monat oder monatlich etwa 498 Angriffe pro Organisation verzeichnet hat. Dies ist eine Steigerung von 10% gegenüber dem Vorjahr und unterstreicht die wachsende Verwundbarkeit von Webanwendungen für Gesundheitsorganisationen, von denen viele immer noch Schwierigkeiten haben, die Anforderungen der anhaltenden globalen Pandemie zu bewältigen.



Während des gesamten Jahres 2020 verwendeten Cyberkriminelle eine Reihe von Vektoren, um gefährdete Gesundheitsorganisationen anzugreifen. Die Hauptziele waren Einrichtungen in den USA, Brasilien, Großbritannien und Kanada.

Im Dezember stellten Imperva Forscher fest, dass vier spezifische Angriffsarten das Volumen der aufgezeichneten Angriffe signifikant erhöhten:

- XSS-Angriffe (Cross-Site Scripting) nahmen im Dezember um 43% zu und stellen die größte Anzahl aller Angriffe da.
- SQL-Injections (SQLi) stiegen um 44% und stellen das zweitgrößte Angriffsvolumen da.

- Protokollmanipulationsangriffe nahmen am stärksten zu (76%) und stellen das drittgrößte Volumen der Gesamtangriffe da.
- RCE / RFI-Angriffe (Remote Code Execution / Remote File Inclusion) nahmen im Dezember um 68% zu, verzeichneten jedoch ein geringeres Gesamtangriffsvolumen.

Auswirkungen sind noch unbekannt… Vorerst

Während das Volumen der Angriffe im Jahr 2020 zunahm, zeigen Berichte, dass die Anzahl der Verstöße abnahm. Als jemand, der seit mehr als 20 Jahren im Bereich Cybersicherheit tätig ist, macht dies keinen Sinn. Unsere Hypothese ist, dass viele Organisationen das Ausmaß oder die Auswirkungen dieser Angriffe wahrscheinlich noch nicht kennen. Der Grund dafür war: Während des größten Teils des Jahres konzentrierte sich das Gesundheitswesen darauf, Fernarbeit zu ermöglichen und gleichzeitig die Frontlogistik einer globalen Pandemie zu verwalten. Somit wurde weniger Zeit für die Bedrohungsforschung, die Reaktion auf Vorfälle und die Analyse von Vorfällen aufgewendet.

Wir gehen davon aus, dass im neuen Jahr viele Angriffe auf Daten wieder auf ihren Ursprung zurückkehren werden. Es gibt auch einige frühe Beweise, die diese Vorhersage stützen. In nur den ersten drei Tagen des Jahres 2021 verzeichneten die Imperva Forscher einen dramatischen Anstieg des Datenverlusts um 43%, der unbefugten Übertragung von Daten innerhalb eines Unternehmens an ein externes Ziel oder einen externen Empfänger, was häufig auf einen Verstoß zurückzuführen ist.

Mit der Transformation der IT im Gesundheitswesen erweitert sich die Bedrohungslandschaft

Im vergangenen Jahr wurde die IT-Transformation in allen Branchen beschleunigt, um den Herausforderungen der globalen Pandemie gerecht zu werden. Im Gesundheitswesen beschleunigte sich die digitale Agenda in erstaunlichem Tempo. Nach einigen Schätzungen wird das, was normalerweise 10 Jahre dauern würde, nun in drei Jahren erledigt sein. Ich habe sogar von digitalen Initiativen mit einem Zeitplan von Wochen oder Monaten gehört!

Von der Erweiterung der Verfügbarkeit von Telemedizin bis zur Verbesserung des Patientenerlebnisses durch mehr digitale Kanäle hat die Gesundheitsbranche mehr Cloud-basierte Technologien und Anwendungen eingeführt, um diese Ziele zu erreichen. Aufgrund unserer Erfahrung verlassen sich viele Gesundheitsorganisationen jederzeit auf Anwendungen von Drittanbietern, anstatt ihre eigenen zu schreiben, um die Risiken und Kosten der IT-Entwicklung zu verringern und eine bessere Zusammenarbeit zu ermöglichen. Anwendungen von Drittanbietern bieten manchmal geschäftliche Vorteile. Zu den Risiken gehören: Patchen nur auf der Zeitachse des Anbieters, bekannte Exploits, die weit verbreitet sind, und ständige Zero-Day-Forschung zu häufig verwendeten Tools und APIs von Drittanbietern.

Das Vertrauen in JavaScript-APIs und Anwendungen von Drittanbietern führt zu einer Bedrohungslandschaft komplexerer, automatisierter und opportunistischer Cybersicherheitsrisiken, deren Erkennung und Beendigung für alle Unternehmen immer schwieriger wird. Und während Ransomware-Angriffe häufig Organisationen des Gesundheitswesens in den Nachrichten landen, ist es nur das anfällige Anwendungs-Frontend für alle Gesundheitsdaten, das die Vielfalt und das Volumen der oben genannten täglichen Angriffe aufweist.

Verteidigung mit der Geschwindigkeit automatisierter Angriffe

Während diese neuesten Bedrohungsinformationen ein düsteres Bild zeichnen, können Gesundheitsorganisationen heute Maßnahmen ergreifen, um sich selbst zu schützen:

- **Schützen Sie Daten - und alle Wege dorthin.** Mit zunehmender Geschwindigkeit der digitalen Transformation befinden sich Daten an mehr Orten als je zuvor. Da Organisationen des Gesundheitswesens ihre Systeme modernisieren und ihre Dienste über APIs und Anwendungen bereitstellen, besteht für sensible Daten eine weitaus größere Wahrscheinlichkeit, dass sie verfügbar sind. Unternehmen müssen in Anwendungs- und Datensicherheit investieren, um einen mehrschichtigen Schutz zu bieten, der legitimen Datenverkehr ermöglicht und schlechte Akteure fernhält.
- **Entfernen Sie sich von Punktlösungen.** Bei Teams mit unzureichenden Ressourcen ist es unrealistisch, einen wachsenden Stapel von Punktlösungen zu verwalten, um jedes einzelne Risiko anzugehen. Suchen Sie stattdessen einen Partner, der eine integrierte Plattform bietet, die Schutz vor den führenden Angriffen bietet und die Webleistung optimiert, damit das Unternehmen effizienter und sicherer arbeiten kann.
- **Vergessen Sie nicht die Einhaltung gesetzlicher Vorschriften.** Die meisten Datenschutz- und Datensicherheitsbestimmungen verlangen heute von Gesundheitsdienstleistern und Kostenträgern, dass sie Zugangskontrollen und -überwachungen für den gesamten Zugriff auf sensible Gesundheitsinformationen von Patienten nachweisen.

Imperva ist bereit zu helfen, wenn sich die Bedrohungslandschaft ändert

Imperva wird von mehr als 6.200 Kunden auf der ganzen Welt als vertrauenswürdig eingestuft und schützt die Anwendungen, Daten und Websites von Gesundheitsorganisationen vor Cyberangriffen. Mit einem integrierten Ansatz, der Edge-, Anwendungs- und Datensicherheit kombiniert, schützt Imperva Unternehmen in allen Phasen ihrer digitalen Reise. Mit marktführenden Lösungen unterstützt Imperva Gesundheitsorganisationen bei der Einhaltung der unzähligen strengen Datenschutzbestimmungen und -mandate sowie bei der Durchsetzung von Richtlinien, Berechtigungen und Prüfungskontrollen.