Living off the Land: Die neue Angriffsgeneration in der Medizintechnik

Was der Angriff auf Stryker für die gesamte MedTech-Welt bedeutet

„Living off the Land" nutzt vorhandene Werkzeuge für Cyberangriffe © KI generiert von Adlon

Am 11. März 2026 wurde der Medizintechnikhersteller Stryker Ziel eines Angriffs, der ohne jede Schadsoftware auskam. Eine Iran-nahe Gruppe nutzte einzig die vorhandenen IT-Werkzeuge des Unternehmens. Das klingt unspektakulär, zeigt aber einen gefährlichen Trend, der nicht nur die gesamte MedTech-Branche betrifft. Denn Angreifer müssen heute keine Viren mehr einschleusen. Sie nutzen Software, die ohnehin vorhanden ist.

© Adlon

Autor:
Tizian Kohler
Head of Security
Adlon
www.adlon.de

Wirkungsvoller Angriff ohne Schadsoftware

Ein Angriff ohne Schadsoftware – und warum er so wirkungsvoll war: Der Angriff auf Stryker basiert auf einer Methode, die „Living off the Land" genannt wird. Der Begriff beschreibt Angriffe, bei denen Täter keine eigenen Werkzeuge mitbringen, sondern vorhandene nutzen. Die Täter kompromittierten zuerst ein Administrationskonto. Ein solches Konto ist in der IT vergleichbar mit einem Generalschlüssel. Es erlaubt Eingriffe in große Bereiche der Systemlandschaft, u. a. in die Mobile Device Management Lösung des Unternehmens. Danach legten die Angreifer ein neues globales Administrationskonto an und nutzten ein integriertes Fernlöschsystem. Diese Technik heißt „Remote Wipe" und wird normalerweise eingesetzt, um verlorene Dienstgeräte zu löschen.

Bei Stryker wurden damit massenhaft Geräte zurückgesetzt, darunter auch private Smartphones von Mitarbeitenden im BYOD-Programm. Die CISA warnte am 18. März offiziell vor dieser neuen Art von Angriff. Sie betont, dass der Missbrauch von Verwaltungswerkzeugen ein wachsendes Risiko für kritische Infrastrukturen darstellt.

Es betrifft alle

Warum dieser Vorfall die gesamte MedTech-Branche betrifft: Die Medizintechnik ist auf stabile IT-Strukturen angewiesen. Außendienst, Serviceteams, klinische Partner und Lieferketten arbeiten eng vernetzt. Ein Angriff wie bei Stryker betrifft deshalb weit mehr als einzelne Geräte. Wenn hunderte oder tausende Geräte gleichzeitig gelöscht werden, entstehen Ausfälle, die Serviceeinsätze verzögern und Abläufe in Kliniken unterbrechen können.

Bring your own device

Das Konzept „Bring your own device" (BYOD) spielt dabei eine besondere Rolle. BYOD bedeutet, dass Mitarbeitende ihre privaten Smartphones für Arbeitszwecke nutzen. Im Fall Stryker wurden dadurch auch persönliche Fotos, Banking-Apps und eSIMs gelöscht. Das zeigt, wie ein technischer Vorfall schnell emotionale und personelle Konsequenzen entwickeln kann.

Die Regulatorien von NIS2 machen die Abhängigkeit von funktionierender IT zusätzlich sichtbar. Ausfälle können Dokumentationspflichten behindern oder Abstimmungen mit Kliniken beeinträchtigen. Der Stryker-Vorfall ist deshalb kein isoliertes Ereignis, sondern ein Blick in eine Entwicklung, die viele MedTech-Unternehmen betreffen kann.

Was MedTech-Organisationen jetzt tun müssen

Moderne Angriffe richten sich immer häufiger gegen privilegierte Zugänge. Diese Zugänge sind IT-Konten mit besonders weitreichenden

© *Grafik Adlon*

Befugnissen. Werden sie übernommen, können Angreifer die digitalen Werkzeuge des Unternehmens gegen das Unternehmen einsetzen. Der wichtigste Schutz ist deshalb die Begrenzung und Überwachung dieser Berechtigungen. Zero Trust ist dabei ein zentrales Prinzip.

Es lässt sich mit der Hygiene im OP vergleichen. Auch dort wird niemandem allein aufgrund seiner Anwesenheit vertraut. Jeder Schritt wird geprüft und dokumentiert. Übertragen auf die IT bedeutet das: Jeder Zugriff wird kontrolliert und nur das Nötigste erlaubt.

Klare Rollen- und Rechteverteilung

Intune ist in vielen MedTech-Unternehmen das Werkzeug zur Verwaltung von Endgeräten. Es ist ein hilfreiches System, benötigt aber eine klare Rollen- und Rechteverteilung. Dazu gehören Mehr-Faktor-Authentifizierung, zeitlich begrenzte Administratorrechte und die Überwachung ungewöhnlicher Löschbefehle. In Sicherheitsanalysen oder externen Checks (Entra ID Permission Check, NIS2-Readiness Check uvm.) wird sichtbar, dass die meisten Risiken aus falsch vergebenen Berechtigungen entstehen. Ein zentraler Punkt bleibt also: Moderne Angriffe nutzen oft keine Schadsoftware, sondern Funktionen, die eigentlich helfen sollen. Beides zeigt, dass Sicherheit heute vor allem aus der richtigen Konfiguration entsteht.

Fazit

Der Angriff auf Stryker macht deutlich, dass Angreifer für schwere Schäden keine Schadsoftware benötigen. Sie nutzen die Werkzeuge, die Unternehmen für effizientes Arbeiten einsetzen. Deshalb müssen Unternehmen ihre Sicherheitsmechanismen anpassen, denn der moderne digitale Arbeitsplatz kann Schutzschild oder Angriffsfläche sein. Entscheidend ist, wie gut die Schlüsselpositionen geschützt und wie verantwortungsvoll die vorhandenen Werkzeuge eingesetzt werden.

Wer schreibt:

Tizian Kohler ist seit Mai 2025 Head of Security bei ADLON Intelligent Solutions GmbH. Zuvor war er bei der Kriminalpolizei als Referent für Cybercrime und Digitale Spuren tätig. Seine Expertise umfasst Netzwerksicherheit, Cloud-Security, Incident Response und digitale Forensik. Mit dieser einzigartigen Kombination aus polizeilicher Cybercrime-Erfahrung und Unternehmensberatung bringt er praxisnahe und compliance-orientierte Perspektiven in die Sicherheitsstrategie von Unternehmen. ◄

© *Adobe Stock, Firefly, generiert für Adlon*