NULLWIRE SECURITY

NULLWIRE SECURITY · SICHERHEITSBEWERTUNG & RETAINER

Penetrationstest des Portals

Eine umfassende Red-Team-Bewertung des Patientenportals, unterstützt durch ein Breach-Response-Abonnement – entwickelt für HIPAA-regulierte Infrastruktur.

2026

01

DIE CHANCE

Das Patientenportal von Meridian Health Systems verwaltet mittlerweile Laborergebnisse, Abrechnungen und Nachrichten für 340.000 Patienten – und wurde noch nie einem externen Red-Team-Assessment unterzogen. Dies ist der Plan, es ordentlich zu testen und vorbereitet zu sein, falls etwas durchdringt.

WARUM JETZT

Das Patientenportal von Meridian Health Systems hat sich von einem einfachen Terminplaner zum primären Kanal für Laborergebnisse, Abrechnung und sichere Nachrichten im gesamten Krankenhausnetzwerk entwickelt. Es wird vierteljährlich intern auf bekannte Schwachstellen gescannt, stand jedoch noch nie einem externen Angreifer gegenüber, der kleine Schwachstellen so verkettet, wie es ein echter Angreifer tun würde – und ein durchschnittlicher Datenschutzvorfall im Gesundheitswesen wird immer noch erst nach über 200 Tagen entdeckt.

Nullwire Security schlägt ein achtwöchiges Engagement vor, das einen umfassenden Penetrationstest – extern, intern und Social Engineering – mit einem laufenden Breach-Response-Abonnement kombiniert, sodass Meridian vor einem Vorfall getestet und während eines Vorfalls reaktionsbereit ist. Die folgenden Abschnitte erläutern den Ansatz, den Leistungsumfang, den Zeitplan und die Investition.

01
140+
DURCHGEFÜHRTE PENETRATIONSTESTS

02
<4 Std.
MITTLERE AKTIVIERUNGSZEIT BEI SICHERHEITSVORFÄLLEN

03
8 Wochen
VON DER SCOPE-FESTLEGUNG BIS ZUM ABSCHLUSSBERICHT

DIE HERAUSFORDERUNG

Interne Schwachstellenscans erkennen bekannte CVEs, übersehen jedoch verkettete Exploits, falsch konfigurierte Drittanbieter-Integrationen und die menschlichen Schwachstellen, auf die eine Phishing-Kampagne abzielen würde. Die Labor-Ergebnis-API und die Anbindung des Abrechnungsdienstleisters von Meridian wurden noch nie unabhängig geprüft.

Operativ wurden Erkennung und Reaktion noch nie anhand eines realen Szenarios geprobt. Käme es tatsächlich zu einem Sicherheitsvorfall, wäre der vorliegende Incident-Response-Plan ungetestet, und dem Team ist nicht bekannt, wie lange die Eindämmung tatsächlich dauern würde.

UNSER ANSATZ

Wir führen das Engagement so durch, wie es ein echter Angreifer tun würde: externe Aufklärung und Exploitation, laterale Bewegung von einem simulierten kompromittierten Endpunkt aus sowie eine Social-Engineering-Kampagne gegen den Helpdesk, ergänzt durch eine gezielte Prüfung der beiden Drittanbieter-Integrationen, über die Patientendaten laufen.

Die Ergebnisse werden direkt der HIPAA Security Rule zugeordnet und mit einem Nachtest zur Behebung zurückgegeben, sodass nichts als abgeschlossen markiert wird, bevor die Behebung verifiziert ist. Das Breach-Response-Abonnement hält anschließend dasselbe Team einsatzbereit, sodass der nächste Vorfall geprobt statt improvisiert abläuft.

01 EXTERNER PENETRATIONSTEST

Internetzugängliche Systeme, das Patientenportal und dessen öffentliche APIs, bis zur Ausnutzung getestet.

02 INTERNE & LATERALE BEWEGUNG

Ein simuliertes Szenario eines kompromittierten Endgeräts, das testet, wie weit sich ein Angreifer nach dem Eindringen bewegen könnte.

03 SOCIAL ENGINEERING

Eine Phishing-Simulation und eine Pretexting-Kampagne gegen den Helpdesk bei Mitarbeitenden.

04 PRÜFUNG DER DRITTANBIETER-INTEGRATIONEN

Sicherheitsbewertung der API-Verbindungen zu Laborergebnis- und Abrechnungsdienstleistern.

05

RETAINER FÜR DIE REAKTION AUF SICHERHEITSVORFÄLLE

Rufbereite Vorfallreaktion und ein geprobtes, einsatzbereites Runbook für Sicherheitsvorfälle.

06

COMPLIANCE-BERICHTERSTATTUNG

Ergebnisse direkt der HIPAA Security Rule zugeordnet für Audits und Berichte an den Vorstand.

> **Nullwire hat eine verkettete Schwachstelle gefunden, die unser internes Team zwei Jahre lang übersehen hatte, und uns beim realen Test des Retainers innerhalb einer Stunde unter Kontrolle gebracht.**

OWEN MARSH

STATUS

REGISTRIERUNGEN, VERSICHERUNGSSCHUTZ UND NACHWEISE

NACHWEIS	AUSSTELLENDE STELLE	REFERENZ	UMFANG	STATUS
Eingetragene Gesellschaft	Handelsregister, Vereinigte Staaten	Nullwire Security LLC	Handelsname und Rechtsform	Aktiv
Steuerliche Registrierung	Finanzbehörde, Vereinigte Staaten	EIN 91-4820376	Alle in Rechnung gestellten Leistungen	Aktiv
Berufshaftpflichtversicherung	Gewerblicher Versicherer	Auf Anfrage erhältlich	Sicherheitsbewertung & Bereitschaftsvertrag	Wird jährlich erneuert
Betriebshaftpflichtversicherung	Gewerblicher Versicherer	Auf Anfrage erhältlich	Arbeiten vor Ort und in den Räumlichkeiten des Kunden	Wird jährlich erneuert
Mitgliedschaft in einem Branchenverband	Branchenverband, Vereinigte Staaten	Auf Anfrage erhältlich	Verhaltenskodex und Beschwerdeverfahren	In gutem Rechtsstand

Zertifikate und Versicherungsnachweise werden auf Anfrage zur Verfügung gestellt und werden Meridian Health Systems auf Anfrage jederzeit während des Auftrags erneut ausgestellt.

[01] ▸ WOCHEN 1–2 · SCOPING & AUFKLÄRUNG

Regeln des Engagements, Erfassung der Assets und Mapping der Angriffsfläche.

[02] ▸ WOCHEN 3–5 · AKTIVE TESTS

Externe, interne und Social-Engineering-Tests gemäß vereinbartem Umfang.

[03] ▸ WOCHE 6 · ERGEBNISSE & HIPAA-MAPPING

Konsolidierung der Ergebnisse und Zuordnung zu den relevanten Schutzmaßnahmen der HIPAA Security Rule.

[04] ▸ WOCHE 7 · UNTERSTÜTZUNG BEI DER BEHEBUNG

Begleitete Unterstützung des Engineering-Teams bei der Behebung vor dem Nachtest.

01
BEWERTUNG
$94,000

- Vollständiges achtwöchiges Engagement
- Externe, interne und Social-Engineering-Tests
- HIPAA-zugeordneter Befundbericht
- Zwei Wochen Unterstützung bei der Behebung

02
BEWERTUNG + RETAINER
$6,500/mo

- Alles aus Assessment
- Rund um die Uhr erreichbare Hotline für Sicherheitsvorfälle
- Monatlicher erneuter Schwachstellenscan
- Priority-SLA für die Reaktion auf Sicherheitsvorfälle [<4 Std.]

03
KONTINUIERLICHE VERTEIDIGUNG
$13,000/mo

- Alles aus Retainer
- Vierteljährliche Red-Team-Übungen
- Kontinuierliche Überwachung der externen Angriffsfläche
- Eingebettete Zeit für Sicherheitsentwicklung

GESCHÄFTSMODELL

WIE SICH DIE DREI STUFEN VERGLEICHEN

	BEWERTUNG	BEWERTUNG + RETAINER	KONTINUIERLICHE VERTEIDIGUNG
Preis	$94,000	$6,500/mo	$13,000/mo
Kernumfang	Vollständiges achtwöchiges Engagement	Alles aus Assessment	Alles aus Retainer
Was enthalten ist	Externe, interne und Social-Engineering-Tests	Rund um die Uhr erreichbare Hotline für Sicherheitsvorfälle	Vierteljährliche Red-Team-Übungen

Lieferung	HIPAA-zugeordneter Befundbericht	Monatlicher erneuter Schwachstellenscan	Kontinuierliche Überwachung der externen Angriffsfläche
Nachbetreuung	Zwei Wochen Unterstützung bei der Behebung	Priority-SLA für die Reaktion auf Sicherheitsvorfälle (<4 Std.)	Eingebettete Zeit für Sicherheitsentwicklung

Die Preise verstehen sich in USD zzgl. der Umsatzsteuer (wa — freiberufliche Dienstleistungen befreit). Optionen können kombiniert oder gestaffelt werden; die Empfehlung für Meridian Health Systems ist im Preisabschnitt hervorgehoben.

DAS ANLIEGEN

AN DER FINANZIERUNGSRUNDE TEILNEHMEN

Wir nehmen Kapital auf, um die auf der vorherigen Seite dargestellte Roadmap zu finanzieren. Nullwire Security würde sich über ein Folgegespräch in diesem Quartal freuen.

Genehmigen Sie diesen Vorschlag, und wir reservieren einen Scoping-Start für die Woche vom 16. Februar. Antworten Sie auf dieses Dokument oder schreiben Sie eine E-Mail an contact@nullwiresecurity.com.

Nullwire Security
contact@nullwiresecurity.com · +1 206 555 0189 · nullwiresecurity.com · Seattle, WA 98109