NULLWIRE SECURITY

NULLWIRE SECURITY — SICHERHEITSBEWERTUNG & RETAINER

# Anforderungsspe

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



2026

# INHALT



AUF EINEN BLICK

# DOKUMENTENKONTROLLE

01
SPEZIFIKATION
**REQ-2026-0771**
Ausgestellt am 22. Januar 2026

02
ERSTELLT VON
**Nullwire Security**
Seattle, WA 98109

03
INHABERIN
**Renata Cole**
Leiter Informationssicherheit, Meridian Health Systems

04
STATUS
**Zur Prüfung**
Baseline bei Genehmigung festgelegt

05
ANFORDERUNGEN
**8**
Funktional und nicht-funktional

01

# EINFÜHRUNG & UMFANG

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.

## ZWECK & ZIELGRUPPE

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.

## FUNKTIONALE ANFORDERUNGEN

| ID | ANFORDERUNG | PRIORITÄT |
|---|---|---|
| R-01 | Externe und interne Tests müssen das Patientenportal und seine zwei benannten Drittanbieter-Integrationen umfassen | MUSS |
| R-02 | Testkonten und ein unterschriebenes Rules-of-Engagement-Schreiben werden vor Testbeginn bereitgestellt | MUSS |

| | | |
|---|---|---|
| R-03 | Alle Feststellungen werden der jeweiligen HIPAA-Security-Rule-Schutzmaßnahme zugeordnet | MUSS |
| R-04 | Kritische und hohe Feststellungen werden vor der endgültigen Abnahme erneut getestet und als geschlossen verifiziert | MUSS |
| R-05 | Die Social-Engineering-Kampagne beschränkt sich auf den Helpdesk und benannte Abteilungen | MUSS |
| R-06 | Das Runbook für die Vorfallsreaktion enthält definierte Rollen und ein 4-Stunden-Aktivierungs-SLA | SOLLTE |
| R-07 | Es werden keine Produktions-Patientendaten exfiltriert oder über Proof-of-Concept-Screenshots hinaus aufbewahrt | MUSS |
| R-08 | Der Abschlussbericht wird sowohl in einer Management- als auch in einer technischen Detailfassung geliefert | SOLLTE |

| ID | PRIORITÄT | ANFORDERUNG |
|---|---|---|
| R-01 | Muss | Externe und interne Tests müssen das Patientenportal und seine zwei benannten Drittanbieter-Integrationen umfassen |
| R-02 | Muss | Testkonten und ein unterschriebenes Rules-of-Engagement-Schreiben werden vor Testbeginn bereitgestellt |
| R-03 | Muss | Alle Feststellungen werden der jeweiligen HIPAA-Security-Rule-Schutzmaßnahme zugeordnet |

| | | |
|---|---|---|
| R-04 | Muss | Kritische und hohe Feststellungen werden vor der endgültigen Abnahme erneut getestet und als geschlossen verifiziert |
| R-05 | Muss | Die Social-Engineering-Kampagne beschränkt sich auf den Helpdesk und benannte Abteilungen |

### 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.

SPEZIFIKATION

# KOMPONENTENSPEZIFIKATION

| REF. | POSITION | SPEZIFIKATION | EINHEITEN | VORLAUFZEIT | EINZELPREIS |
|---|---|---|---|---|---|
| SPC-01 | Scoping & Aufklärung | Regeln des Engagements, Erfassung der Assets und Mapping der Angriffsfläche | 2 | 2 Wo. | $9,500 / wk |
| SPC-02 | Externer Penetrationstest | Bewertung des internetzugänglichen Patientenportals und der API | 2 | 2 Wo. | $14,000 / wk |
| SPC-03 | Interne & Social-Engineering-Tests | Simuliertes Szenario mit kompromittiertem Endpunkt und Phishing-Übung | 1 | 1 Wo. | $16,000 / wk |
| SPC-04 | Prüfung der Drittanbieter-Integrationen | Sicherheitsbewertung der API von Labor-Ergebnis- und Abrechnungsdienstleistern | 1 | 1 Wo. | $12,000 / wk |
| SPC-05 | Berichterstattung & Unterstützung bei der Behebung | Ergebnisbericht, HIPAA-Mapping und Anleitung zur Behebung | 1 | 1 Wo. | $10,000 / wk |
| SPC-06 | Retest & Einrichtung Retainer | Erneute Prüfung der Fehlerbehebung und Übergabe des Breach-Response-Runbooks | 1 | 1 Wo. | $9,000 / wk |

Die Spezifikationen werden mit der Abnahme festgelegt; jede Änderung wird über das in diesem Dokument beschriebene Änderungsverfahren abgewickelt.

[01]

## TESTS AUF ANGREIFERNIVEAU

Externe, interne und Social-Engineering-Tests, verkettet, wie es ein echter Angreifer tun würde.

[02]

## HIPAA-ZUGEORDNETES REPORTING

Jeder Befund der relevanten Sicherheitsmaßnahme der HIPAA Security Rule zugeordnet, bereit für Audit und Berichterstattung an den Vorstand.

[03]

## STÄNDIGE EINSATZBEREITSCHAFT

Ein eingeübtes Runbook für die Reaktion auf Sicherheitsvorfälle und ein Bereitschaftsdienst, sodass der nächste Vorfall geübt statt improvisiert abläuft.

[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.

# NULLWIRE SECURITY

500 Yale Ave N, Seattle, WA 98109, United States

contact@nullwiresecurity.com · +1 206 555 0189 · nullwiresecurity.com

Nullwire Security LLC · EIN 91-4820376