Cyberangriff auf den externen Abrechnungsdienstleister

29.05.2026, 11:30 | IT, New Media & Software

Pressemitteilung von: *Darkscope*

Firmenlogo

Der aktuelle Cyberangriff auf den externen Abrechnungsdienstleister mehrerer deutscher Universitätskliniken zeigt ein wachsendes strukturelles Problem: Risiken entstehen heute zunehmend innerhalb digitaler Lieferketten und externer Dienstleister — nicht mehr nur in der eigenen IT.

Obwohl die Kliniken selbst nicht direkt kompromittiert wurden, könnten sensible Daten von zehntausenden Patienten betroffen sein. Der Vorfall verdeutlicht, dass Unternehmen ihre interne IT besser absichern, gleichzeitig aber die Kontrolle über Risiken in komplexen Drittparteien-Strukturen verlieren.

Im Rahmen einer externen Analyse identifizierte das Cyber-Intelligence-Unternehmen Darkscope bei öffentlich erreichbaren Systemen unter anderem eine große externe Angriffsfläche, erkennbare Schwachstellen, exponierte Dienste sowie Hinweise auf frühere Datenleaks und Darknet-Erwähnungen rund um die Marke „Unimed“. Solche Informationen erhöhen häufig die Sichtbarkeit einer Organisation innerhalb krimineller Ökosysteme und können Folgeangriffe begünstigen.

Die eigentliche Herausforderung moderner Lieferketten liegt in fehlender Transparenz über Abhängigkeiten, Sub-Lieferanten und kritische Geschäftsprozesse. Klassische Third-Party-Risk-Management-Ansätze mit Audits, Fragebögen und Excel-Listen stoßen zunehmend an ihre Grenzen. Mit NIS2 und DORA steigen die Anforderungen zusätzlich. Unternehmen müssen Risiken, kritische Drittparteien und Abhängigkeiten künftig kontinuierlich überwachen. Third-Party Risk Management wird damit zu einem zentralen Faktor für operative Resilienz und Geschäftsfortführung. Und auch zu einem Faktor für zukünftige Sicherheit und Ausfallsicherheit der Firmen in der Zukunft.

Andre Weihrauch

Darkscope

www.360tprm.de

Darkscope

Gutsweg 1
Dargelin 17498
Deutschland

AndreWeihrauch (General Manager Europe)

01629209108

andre.weihrauch@darkscope.com

www.360tprm.de

Portrait

Darkscope ist ein international tätiges Cyber-Intelligence-Unternehmen mit Fokus auf KI-gestützte Bedrohungsanalyse, Dark-Web-Monitoring und kontinuierliche Cyber-Risikobewertung. Das Unternehmen unterstützt Organisationen dabei, potenzielle Angriffe frühzeitig zu erkennen, kompromittierte Daten aufzuspüren und Risiken entlang der gesamten digitalen Angriffsfläche sichtbar zu machen.

Mit eigenen KI-Technologien und sogenannten „Seekers“ analysiert Darkscope Daten aus dem Internet, sozialen Netzwerken, Foren, Messenger-Kanälen und dem Dark Web in Echtzeit. Zu den zentralen Lösungen gehören unter anderem Cyber Threat Sentinel, Cyber Watchtower sowie CIQ360 zur Bewertung von Partner- und Lieferantenrisiken im Kontext von NIS2, DORA und Third-Party-Risk-Management.

Darkscope arbeitet international mit Unternehmen aus unterschiedlichen Branchen zusammen und verbindet moderne Cyber Threat Intelligence mit praxisnaher Risikoanalyse, um Sicherheitsverantwortlichen, Management und Compliance-Teams fundierte Entscheidungsgrundlagen zu liefern

News-ID: 1313205 • Views: 243 (Stand: 26.08.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/1313205/Cyberangriff-auf-den-externen-Abrechnungsdienstleister.html