Press Release

報道関係各位

SecurityScorecard株式会社
2024年7月8日

※本リリースは、米国時間2024年6月25日に米国SecurityScorecardより発表されたプレスリリースの抄訳です。

SecurityScorecard「米国ヘルスケア業界サイバーリスク脅威調査 2024」ヘルスケア業界のサイバーセキュリティ評価は「B+」
- サプライチェーン関連のサイバーリスクという重大な脆弱性に直面 -

SecurityScorecard株式会社（本社：米国、ニューヨーク州、CEO：アレクサンドル・ヤンポルスキー、以下SecurityScorecard、日本法人代表取締役社長　藤本 大）は、2024年6月25日に最新レポート「米国ヘルスケア業界サイバーリスク脅威調査 2024」（英文のみ）を発表し、2024年上半期のヘルスケア業界のサイバーセキュリティ評価が「B+」であることを明らかにしました。また、ヘルスケア業界がサプライチェーンのサイバーリスクという重大な脆弱性に直面していることを指摘しています。
さらに、このレポートでは、過去のデータ侵害とセキュリティ評価を詳しく調査し、ヘルスケア業界がサプライチェーンにおける侵害を阻止するためのインサイトを提供しています。

SecurityScorecard の Threat Research, Intelligence, Knowledge, and Engagement (STRIKE) チームは、Change Healthcare社のランサムウェア攻撃を受けて、米国の大手ヘルスケア企業500社が直面する最も重大なリスクを調査しました。

主な調査結果

- **ヘルスケア業界の評価は B+**
  2024年上半期の米国ヘルスケア業界のセキュリティ評価は予想を上回り、平均スコアは「88」となりました。しかし、改善の余地は依然として残されています。評価「B」の組織は、評価「A」の組織よりもデータ侵害の被害に遭う可能性が2.9倍高いことが明らかになっています。

- **ヘルスケア業界はサードパーティによる情報漏えい被害が最多**
  2023年に起こったサードパーティによる情報漏えい被害の35%が医療関連組織を対象としており、他のどの業界よりも高い割合となっています。ヘルスケア業界におけるサプライヤーエコシステムは、ランサムウェアグループにとって非常に魅力的なターゲットです。攻撃者は、1つの脆弱性を悪用して何百もの組織に侵入し、検出されることなく活動することができます。

- **医療用機器関連企業は侵害リスクが高**
  医療用機器および医療用設備企業は、サイバーセキュリティのスコアが医療業界全体の平均と比較して2～3ポイント低いことが判明しました。また、これらの企業は他の医療セクターと比較して、侵害された機器や侵害の報告率が16%高くなっています。

- **AppSec は攻撃ターゲットにおける最大の脅威**

アプリケーションセキュリティ（AppSec）の課題は、医療業界における攻撃ターゲットで最も重大な欠陥の一つです。このカテゴリーで最低スコアを記録した組織の48%がヘルスケア関連企業に該当します。ソフトウェア上のサプライチェーンは、攻撃者にソースコード、ビルドプロセス、パイプラインツール、またはソフトウェアアップデートへのアクセスを可能にし、攻撃をサプライヤーの顧客にまで拡大します。サプライヤーとそのシステムを暗黙的に信頼している顧客は少なくありません。

- **脅威の高まりにもかかわらず、公表されている侵害件数は少ない**
  医療関連組織の5%が過去1年間に公表された侵害を経験しており、6%は過去30日間にネットワーク上の機器に侵害された形跡がありました。ランサムウェアは、依然としてヘルスケア業界にとって最大の脅威となっています。

集中するサイバーリスク
Change Healthcare社の被害により、一部の企業は1日あたり100万ドルもの損失を被っています。この結果、企業のセキュリティ担当役員は、サプライヤーの監督とサイバーセキュリティ対策を強化する取り組みを進めています。すべての組織は、データセキュリティ対策の精査、機密データへのサードパーティおよびフォースパーティのアクセス評価、収益に関わる重要なベンダーの特定を行う必要があります。

SecurityScorecardの 脅威調査・情報担当上級副社長 ライアン・シェルトビトフ氏は、次のように述べています。
「医療請求処理を支えていたChange Healthcare社のようにたった一つでも脆弱なポイントが存在する場合、医療エコシステム全体が機能不全に陥る可能性があります。サイバーセキュリティコミュニティがサプライチェーンのリスクを積極的に監視しなければ、歴史は繰り返されるでしょう。私たちは力を合わせて、たった一か所であっても、攻撃に悪用される可能性のあるポイントを特定し、対処しなければなりません」

調査方法
この調査では、米国で株式が公開取引されている医療関連企業500社のセキュリティ評価と過去のセキュリティ侵害データを調査しています。

その他のリソース
- 「米国ヘルスケア業界サイバーリスク脅威調査 2024」のダウンロードはこちらを御覧ください。
- SecurityScorecardの脅威インテリジェンスについて詳しくは、弊社ウェブサイトをご覧ください。

SecurityScorecard のThreat Research, Intelligence, Knowledge, and Engagement (STRIKE) チームについて
独自の脅威インテリジェンス、インシデント対応の経験、サプライチェーンのサイバーリスクに関する専門知識を兼ね備えています。SecurityScorecardのテクノロジーに支えられたSTRIKEチームは、世界中のCISOの戦略的アドバイザーとなり、STRIKE チームによる脅威調査を基に、組織にサプライ チェーンのサイバー リスクと攻撃者の特性に関してアドバイスを行っています。

SecurityScorecardについて

Evolution Equity Partners、Silver Lake Partners、Sequoia Capital、GV、Riverwood Capitalなど、世界トップクラスの投資家が出資するSecurityScorecardは、サイバーセキュリティの格付け、対応、回復力におけるグローバルリーダーであり、1200万社以上の企業が継続的に格付けを受けています。
セキュリティとリスクの専門家であるアレクサンドル・ヤンポルスキー博士とサム・カッスーメによって2013年に設立されたSecurityScorecardの特許取得済みセキュリティレーティングテクノロジーは、企業のリスク管理、サードパーティリスク管理、取締役会報告、デューデリジェンス、サイバー保険の引き受け、規制当局の監視のために25,000以上の組織で使用されています。
SecurityScorecardは、企業におけるサイバーセキュリティ・リスクの理解、改善を促進し、取締役会、従業員、ベンダーに伝える方法を変革することで、世界をより安全にすることを目指します。SecurityScorecardは、Federal Risk and Authorization Management Program (FedRAMP) Readyの指定を受け、顧客情報を保護するための同社の強固なセキュリティ基準を強調し、米国のCybersecurity & Infrastructure Security Agency (CISA)によって無料のサイバーツールおよびサービスとして登録されています。すべての組織は、信頼性と透明性の高いInstant SecurityScorecardの評価を受ける普遍的な権利を有しています。
www.securityscorecard.com/jp/

日本法人社名 ：　SecurityScorecard株式会社（セキュリティスコアカード）
本社所在地 ：　東京都千代田区丸の内一丁目 1 番 3 号
代表取締役社長 ：　藤本 大

【本件に関する連絡先】
SecurityScorecard
広報代理店 株式会社プラップジャパン
担当　菊池(070-2161-7123)、牟田(090-4845-9689)、冨安(070-2161-6963)
Email: securityscorecard@prap.co.jp