Press Release

報道関係各位

SecurityScorecard株式会社
2023年12月13日

SecurityScorecard、2024年 サイバーセキュリティに関する予測を発表

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 サイバーセキュリティに関する予測」を発表しました。2024年、「サイバーセキュリティに特化した言語モデルの台頭」、「攻撃者によるAIのより一層の悪用」、「記録的な数の顧客情報漏えい」、「組織がサイバーセキュリティを重視」など、2024年度のサイバーセキュリティに関する予測をしています。

2024年サイバーセキュリティに関する予測

共同設立者兼CEO:アレクサンドル・ヤンポルスキー

小規模でも強力：サイバーセキュリティ特化型言語モデルの台頭

大規模言語モデル(LLM)は、組織におけるサイバーセキュリティに変革をもたらしました。LLMはシンプルなクエリを実行することで、山のようなデータから実用的な洞察を導きだす驚異的パワーをセキュリティチームにもたらしました。しかし、LMM はゲームチェンジャーである一方、サイバーセキュリティ特有のデータセットの複雑さを理解するには限界があり、多くの場合、担当者はビジネス特有の課題に苦戦を強いられていれます。

2024年、セキュリティチームは小規模言語モデルに移行する可能性があります。これらのアジャイルで特化したモデルは、LLMが突きつける障壁を打ち破り、カスタマイズされた実用的なインサイトを提供していくと見られます。リアルタイムデータトレーニングが武器となり、セキュリティチームは刻一刻と変化する脅威の状況に迅速に対応可能になると予測しています。

2024年のAI戦争は、攻撃者が勝利

生成AIの台頭により、重要な議論が巻き起こりました。それは、組織が生成AIを迅速に活用するのか、それとも攻撃者が生成AIを速やかに悪用して優位に立つのかという議論です。残念ながら、攻撃者側が生成AIの導入で組織を先回り、ダークサイド側が先行すると見られます。このことから、ディープフェイク、巧妙なフィッシングキャンペーン、エンドポイントセキュリティの防御を回避するステルス型のペイロードなど、容赦ない攻撃に備えるべきです。これらの課題は、かつてないほどサイバーセキュリティの防御が試されることになると予測しています。

2024年には、主要な第三者による情報漏洩事件が発生、記録的な数の顧客データが漏えい

2024年、サードパーティによる情報漏えいの大波が押し寄せることが予測されます。サイバー犯罪者が価値の高いターゲットに狙いを定める中、大量の顧客基盤を持つ大手ハイテク企業がこの嵐の矢面に立たされることになると見られます。APIの普及からデータのデジタル化まで、様々な要因が重なり、サードパーティーリスクの温床となっています。これらのリスクを測定・管理するための明確なKPIを設定し、実施するための早急な対策を取るべきです。

2024年、取締役会はサイバーセキュリティに注目

証券取引委員会の画期的なサイバー規制により、取締役会はサイバーセキュリティにスポットライトを当てることを余儀なくされると見られます。SEC(米国証券取引委員会) の情報開示要件により、最高情報セキュリティ責任者(CISO)は取締役会のメンバーと有意義な議論を行い、サイバーセキュリティのリテラシーを高めるように注力していきます。取締役会のメンバーが粗利率のような財務の概念を理解するのと同様、今後は、サイバーセキュリティがビジネスに与える影響について技術的な理解を深めることになるでしょう。取締役会がサイバーリテラシーを受け入れることにより、サイバーレジリエンスは現実のものとなると予測されます。

最高情報セキュリティ責任者（**CISO**）スティーブ・コブ

ベンダーのセキュリティ評価をアンケートのみで行っている組織は、第三者による情報漏えいが発生する可能性が**3**倍高く

MOVEitの脆弱性により生じた直近の衝撃は、サイバー攻撃はたとえ強力なセキュリティ対策を誇る組織であっても容赦されない、という事実を実証したことです。98%の企業が少なくとも侵害経験のあるベンダー1社と関係を持つ中、サードパーティーリスクが懸念される新時代においてベンダーを適切に評価するには、従来のチェックリストのアプローチでは不十分です。

大半のベンダーは、アンケートに振り回され、自社のセキュリティプログラムを深く掘り下げるスキルもリソースもないまま、慌ただしくプロセスを進め、チェックボックスにチェックを入れるだけとなっています。2024年、セキュリティチームとベンダーは、敵対者としてではなく、デジタルエコシステム全体のリスクを特定、管理する使命を担うパートナーとして協力しあうことになると見られます。表面的なアンケートの時代は、堅牢なセキュリティエコシステムを構築するための積極的な取り組みに変わり、真のサイバーセキュリティレジリエンスには、進化する脅威に対して団結して立ち向かうことが必要と認識されることが予測されます。

技術的なサイバーセキュリティリスクをビジネス用語に適切に置換できない最高情報セキュリティ責任者**(CISO)**は、職を失う

サイバーセキュリティの世界では、CISO がサイロ化された技術の世界の中だけで活動する時代は終わろうとしています。CISO としての職の存続は、技術的なサイバーセキュリティリスクを、ビジネス上の意思決定が行われる取締役会において理解できる言葉に置換できるかどうかにかかっています。

今後ますます取締役会におけるサイバーセキュリティリスクへの注目は高まることが予測されます。SEC(米国証券取引委員会) の新しいサイバーセキュリティ開示最終規制、最近のSECがSolarWinds とその CISOを告発したニュース 、そして 2023 年を通して絶え間なく続くサイバー侵害は、役員会の議論の的となっています。2024年もサイバーセキュリティがビジネスアジェンダを支配

し続ける中、CISOは適応しなければならず、そのようなセキュリティ上の懸念に効果的に対処できない場合、CISO交代という現実とそれに伴う責任に直面することになると予測されます。

このような危険な海を航海するために、CISOは合理化された反復可能なプロセスを作成するプロフェッショナルとなり、効果的なコミュニケーションを優先しなければならないと見られます。CISOが生き残るためには、最高経営責任者（CEO）や取締役会との対話において、複雑な技術的概念をビジネス陣営が理解できる言語に置換するという重要なスキルにかかっています。それは、単にサイバーについて話すのではなく、適切なセキュリティ投資を怠ることによる財務リスクと風評リスクを明確に伝えることです。時間は刻一刻と迫っており、そうすることができなければ、CISOの職を失することになるのです。

脅威インテリジェンス担当副社長 アレックス・ハイド

攻撃者は**AI**を使ってゼロデイを半分の時間で悪用

攻撃者はAI(人工知能)を活用し、より迅速に行動するようになってきています。2023年に見られるAI導入の急増は、ほんの始まりにしか過ぎません。2024年は、ゼロデイ脆弱性が指数関数的に増加すると予測してされています。攻撃者は、大規模言語モデル（LLM）を悪用して高度なエクスプロイトを作成し、既知のエクスプロイトが判明するまでの平均時間を半減すると見られます。その結果、攻防における熾烈なAI戦争が繰り広げられ、両者とも防御と侵入にテクノロジーを活用することが予測されます。

暗号通貨の衝突：**2024**年のビットコイン半減期におけるサイバーセキュリティに警鐘

長い間、暗号通貨は、その分散型の性質を利用して資金洗浄を行う悪質な行為者の避難所となってきていました。しかし、ビットコインの次の半減イベントが近づく2024年春に注目すべきです。このイベントは4年ごとに発生し、ビットコインの新規作成率が半分になる時期です。これはサイバーセキュリティにとって何を意味するのでしょうか。暗号通貨取引所を標的として、既知の脆弱性を悪用し、このイベントに乗じてフィッシングの手口を使うランサムウェア攻撃の増加が予測されます。

ディスティングイッシュト・エンジニア　ジャレッド・スミス

国家の支援を受ける攻撃者は、ディープフェイクや**AI**による音声なりすましを利用し、**2024**年の米大統領選に向けて広範なソーシャル・エンジニアリング攻撃を仕掛けてくる予測

2024年の米国大統領選挙に向けて、新たな誤報の時代が国民の不信感を高めると見られます。国家の支援を受ける攻撃者は、ディープフェイクやAIの音声偽装などの最先端技術を導入し、偽情報によるキャンペーンを強化する可能性があります。このような取り組みにより、大規模なソーシャル・エンジニアリングの時代が到来し、事実と虚構の境界線が曖昧になるような真実と見まがう誤情報が生み出されることが予想されます。今までにない欺瞞に満ちた情報操作との戦いに備えるべきです。

サードパーティによるサイバーリスクの津波：侵害の**80%**はサードパーティまたはフォースパーティが起因

2024年、SecurityScorecardの脅威研究者は、侵害の80%がサードパーティまたはフォースパーティに起因すると予測しています。2023年は、サードパーティのサイバーリスクがもたらす脅威が迫っていることを痛感する年となりました。一度、広く利用されているソフトウェアを侵害できるようになると、サイバー犯罪者は、数百、数千の組織にアクセスできるようになります。セキュリティの回復力は、エコシステムの中でWeakest Linkと同程度となってしまいます。セキュリティを維持するためには、自社のセキュリティ、ベンダー、さらにはベンダーのベンダーまでを完全に可視化する必要があります。最近のOktaやMOVEitに対する侵害インシデントは、1つのソフトウェアの欠陥による脅威の波及効果の大きさを表しています。

SecurityScorecardについて
SecurityScorecard Inc.は、アメリカのニューヨーク州に本社を置く、2013年に設立されたサイバー セキュリティ レーティングの世界的リーディング カンパニーです。1,000万以上の組織を継続的に評価している特許取得済みのレーティング技術は16,000以上の組織で、自社のリスクマネジメント、サプライチェーン リスク マネジメント、経営陣向けのレポート、サイバー デュー デリジェンス、またサイバー保険の料率算定などに活用されています。自社グループ・取引先のセキュリティ リスクを定量的に可視化し、サイバー攻撃による侵害発生の可能性を低減するための具体的なアクションを促すことにより、世界をより安全な場所にすることを目標にしています。
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: 八代(070-2161-7123)、牟田(090-4845-9689)、冨安（070-2161-6963）
Email: securityscorecard@prap.co.jp