RSA

2024アイデンティティの最新トレンド

AI時代におけるアイデンティティの将来を読み解く

January 2024

RSA.com

目次 .

エグゼクティブサマリー：予測せず、準備せよ . 2

パスワードレス認証はついに 2024 年に現実のものに . 5

攻撃が増加している一方で、より強力な防御策も存在 6

パスワードレス認証の進展は、「セキュリティ」対「利便性」の議論を激化させる 7

フィッシングに対抗するMFAは、同期されたパスキーの利用が増大し、その結果、より多くのパスキーがさらなるセキュリティ侵害を引き起こす可能性がある 7

CIEM が鍵となる . 10

中小企業がCIAMを実装する時期 11

より多くのデータ、よりスマートな意思決定 12

AI は諸刃の剣。2024 年は、より深く切り込む . 14

人と機械－人VS機械ではない 15

もし今ラムサムウェア攻撃が悪いと思う？ 2024 年はどうなる . 17

MFA: 良いニュースと悪いニュース . 19

サービスデスクはユーザーのためのライフラインであり、攻撃者のための標的になってはならない。 22

防御から自己防衛へ 23

機械の台頭 24

法律業界と専門コンサルティングは攻撃の標的に . 26

2024 年、組織はモバイルセキュリティの問題に対応する新たな方法を探す . 28

エグゼクティブサマリー: 予測せず、準備せよ.

激しく変化する中で興味深いことの一つは少し先の未来であれば予測可能であると言えるでしょう。天気を考えてみてください：気象予報士がたまには外すことはあっても、実際には週末までの天気をかなり正確に予測できています。

しかし、数週間先の予報となると、正確な長期的予測を行うことはほぼ不可能です。あまりにも多くの変数や不確定要素があり、どのような手法でも簡単にはいきません。1 ヶ月後には暑いか寒いか？ 1 年後には雨が降るか晴れるか？それを知る唯一の方法は、実際はその時になるまでわかりません。

同じことが、サイバーセキュリティにも当てはまります。顧客、パートナー、アナリスト、および様々な産業の研究者との対話を通じて、90 以上の国で 2,300 人 以上に対するアイデンティティセキュリティの知識、行動、信念に関する調査を行った結果、組織は利用者、デバイス、権限、環境の数が増加することを考慮する必要があることがわかりました。さらに、ご存じの通り、この成長はより大きく、より脆弱な攻撃対象を作り出すことが予測されます。 Identity Defined Security Alliance の「2023 年のデジタルアイデンティティのセキュリティに関するトレンド」調査 によれば、過去 1 年間において 90%の企業がアイデンティティに関連するインシデントを経験し、98%が、管理を必要とするアイデンティティの数が増加していると考えています。

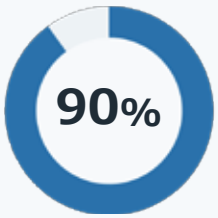
変化のペースはますます加速するでしょう。生成 AI がどのように脅威の精度を高め、それらの脅威に対抗するための新しいサイバーセキュリティの機能を導入しているかを見てください。

多要素認証（MFA）の利用の変遷と、そしてサイバー犯罪者が適応する方法を考えてみましょう。脅威者が IT サービスデスクを新たな標的にするようになり、パスワードレス

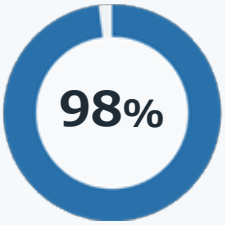
認証の進展によってハッカーの脆弱性が最小限に抑えられる一方で、新しい脆弱性が発見されており、進化がどのような影響を与えているのか認識する必要があります。

以下のセクションでは、攻撃対象の拡大、新しい脅威の方向性、MFA の導入の状況、その他の変化によって生じると見られる新しいリスクの一部について詳細に説明します。RSA のリーダーたちは、これらの新しいリスクに適応するための革新について述べ、AI と共に進化する我々の役割について説明し、サイバー犯罪者がアイデンティティセキュリティの隙間を見つけて攻撃を仕掛ける方法を検証します。私たちは天気を予測しようとしているわけではありません。それが簡単ではないことを知っています。あまりにも多くの変数、相互作用が複雑に絡まり、どの組織もそれに対して完全にコントロールすることは難しい課題です。
しかし、それは無力感を意味するものではありません。それとは逆です。将来を予測できる限界を認めることで、次に何が起こるかに備えることが必要となることがわかるようになるからです。

The Identity Defined Security Alliance' s の 2023 年のデジタルアイデンティティのセキュリティトレンド調査によると：



過去の 1 年間において、90 % の企業がアイデンティティに関連したインシデントが発生



98%が、管理する必要があるアイデンティティの数が増加していると同意

“未来は
パスワードレス
になる.”

パスワードレス認証はついに 2024 年に現実のものに .

「未来はパスワードレスになる」これが、かつてのニューヨーク・タイムズのサイバーセキュリティ記者であるニコール・パールロスが、ユーザーの携帯電話からデスクトップコンピュータに「暗号化されたキーを送信する」新しいイノベーションについて詳細に説明したブログの冒頭です。これにより、「サイトにログインするという時に面倒なプロセス」が少し緩和されます。

パールロスは具体的にいつパスワードレスな未来に到達するかについては詳しく語っていません。明言を避けたことは賢明な判断だと思います。彼女は 2013 年 12 月 18 日にその予測を行いましたが、パスワードレスとパスワードレス認証 は長らく注目されているトピックでありながら、テクノロジー業界は実際には「Something-You-Know」のベース認証を置き換えるためにはほとんど進展していませんでした。もし進展していたなら、データ侵害ははるかに少なかったでしょう。

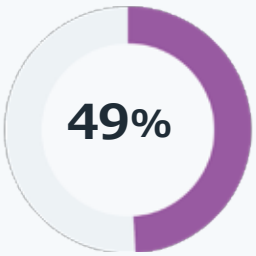
残念ながら、資格情報（特に盗まれたパスワード）は依然として侵害の主要な原因の一つとなっています。 Verizon の 2023 年データ侵害調査レポート によれば、盗まれた資格情報の使用が「侵害の最も一般的な侵入経路になった」とされ、全データ侵害の 49%が資格情報を含んでいました。 Microsoft によれば、パスワード攻撃は「2022 年から 10 倍以上増加し」、月間の攻撃回数が約 30 億から 300 億以上に増加しました。

攻撃が増加している一方で、より強力な防御策も存在

2024 年には、より多くのユーザーがパスワードレス認証を導入することが期待されています。企業は長らくパスワードの不安全性を理解し、パスワードレス認証を採用したかったが、FIDO は消費者向け技術と見なされ、ネイティブプラットフォームサポートにおいてはギャップがあり、実現するのに時間がかかりました。

これらの反対意見は解決されました。パスワードレスの標準は非常に成熟しており、消費者の受け入れにより成長がさらに加速する見通しです。2022 年には、Apple、Google、および Microsoft が「FIDO アライアンスと World Wide Web Consortium によって作成された共通のサインイン標準へのサポートを拡大する計画を発表し、共同の プレスリリース で新しいサポートが「ウェブサイトやアプリがデバイスとプラットフォームを横断して一貫して安全で簡単なパスワードレスのサインインを消費者に提供できるようにする」と述べました。2023 年には、Amazon も広範な取り組みに 参加して パスワードレス認証の推進に加わりました。

2014 年以来、FIDO アライアンス取締役会の主要メンバーであり、同アライアンスのエンタープライズ展開ワーキンググループ（EDWG）、FIDO2 テクニカルワーキンググループ（TWG）、および FIDO ユーザーエクスペリエンスワーキンググループ（UXWG）のメンバーである RSA は、企業がパスワードレス標準に署名することと、技術の受け入れを促進するためにそれを消費者が使用することの両方が重要であることを理解しています。



49%のすべてのデータ侵害が資格情報に関連

Verizon 2023 年データ侵害調査レポート

セキュリティ企業はパスワードレスの必要性を何度も訴えても（我々もそうしています）、そのメッセージは消費者が日常生活でパスワードレスを見て、使って、有効性を享受するか、雇用主がパスワードレス認証を十分に確保できると感じるまで終わりがありません。

ビッグフォーのコミットメント、より成熟した標準、および繁栄するパスワードレスエコシステムは、ついに 2024 年においてパスワードレスに実質的な進展をもたらすでしょう。

パスワードレス認証の進展は、「セキュリティ」対「利便性」の議論を激化させる

全体的には、パスワードレス認証への進展は価値があります。ただし、すべてのパスワードレス認証が同じであるわけではありません。さらに、この進展は新たなリスクと脆弱性を生み出すことになります。

技術の進歩がパスワードレス認証を推進することによって、セキュリティと利便性のどちらを優先するかの議論が考えられます。ビッグ・フォー（主要なテクノロジー企業）が消費者向けにサービスを提供していることを考慮すると、彼らが導入するパスワードレス認証は、おそらく利便性を重視し、これらのパスワードレス認証のパスキーを同期化および管理するためにクラウドプラットフォームに依存する傾向があるでしょう。

逆に、企業はこの議論を異なる視点から見るでしょう。おそらく、企業は引き続きデバイスに結びついたパスキーを使用して高い保証を維持しつつ、認証情報の回復に関するユースケースを改善しようとするでしょう。最終的には、企業はパスキーがどのように管理され、それが彼らのセキュリティの姿勢にどのような影響を与えるかを考慮することになります。

フィッシングに対抗するMFAは、同期されたパスキーの利用が増大し、その結果、より多くのパスキーがさらなるセキュリティ侵害を引き起こす可能性がある

2024 年に認証を変えるのは、単にビッグフォーだけがパスワードレスを支持するだけではありません。 行政命令 M-22-09、「アメリカをゼロトラストサイバーセキュリティの原則に向けて推進」、および FedRAMP によれば、2024 年度末までにフィッシングに対抗する MFA の使用が必要とされます。

2024 年にアメリカ政府がフィッシングに対抗する MFA の使用を義務付ける要件があり、来年においてフィッシングに対抗する MFA の広範な使用につながるであろうと予測することは、地球を揺るがす衝撃的な発見ではありません（我々は同じくらい「来年には太陽が東から昇るであろう」と予測できるでしょう）。

しかし、その要件の影響を検討する必要があります。来年、より多くの政府機関がフィッシングに対抗する MFA を採用するでしょう。政府の要件とビッグ・フォーによるパスワードレスの推進の双方から、多くのユーザーが個人利用のために FIDO 同期パスキーを展開すると予想されます。消費者と企業の両方が、これらのキーがクラウドに同期されることを認識すべきです。我々は、それが起こっていることや、それに伴うリスクを知らないユーザーがいる可能性があると疑っています。前述の通り、同期されたパスキーはセキュリティよりも利便性を優先し、組織に新たな脆弱性を生み出す可能性があります。

政府の要件により、より多くのフィッシングに対抗する機能が展開されることで、我々はより多くの脅威者がユーザーの個人アカウントを標的にし、ユーザーの保管されているパスワードやウォレットを悪用することが予想されます。ユーザーやその組織が特定のパスワードレスの構成やデフォルトを使用している場合、脅威者は侵害された個人アカウントを利用して専門的なリソースに対する攻撃を行う可能性があります。

これは完全に理論的なものではありませんが、昨年、ソフトウェア開発ベンダーの Retool は、27 のクラウド顧客が侵害されたと報告しました。これは主に、「MFA コードをクラウドに同期する Google Authenticator 同期機能」によるものでした。Retool は侵害に関する報告書で、「安全ではなく、Google アカウントが侵害されると、MFA コードも同様に侵害される可能性がある」と述べています。

組織はこれに備えるべきです。特定のユースケースで同期されたパスキーを無効にすることが可能なソリューションを探すことは、パスワードレス認証を安全で便利に保つ手段として非常に価値があります。

“....マルチクラウド構成が
複雑になるほど、
ゼロトラストの実装が
重要.”

CIEM が鍵となる.

ほとんどのビジネスで、ある程度クラウドサービスを利用していることは驚きではないでしょう。 PwC Cloud Business Survey によれば、78% の幹部が「その企業がビジネスのほとんど、またはすべての部分でクラウドを採用している」と述べています。今年、アメリカ政府はクラウドコンピューティングに 90 億ドル を予算化しました。 Gartner は、2025 年までに企業の IT 支出の半分がクラウドに移行すると予測しています。 Identity Defined Security Alliance' s の「2023 年デジタルアイデンティティの保護に関するトレンド」調査によれば、クラウドアプリケーションの増加が回答者全体でアイデンティティ数の増加を推進する最も重要な要因でした。

クラウドへの移行の理由はたくさんあり、すべてを列挙するつもりはありません。しかし、管理されたサービスの利用に伴う利点が多い一方で、組織はクラウド環境がリスクを拡大させることも理解する必要があります。Gartner のレポートを引用した Venture Beat では、「マルチクラウド構成が複雑になるほど、ゼロトラストの実装が難しくなる」と報じています。

そのデータはその通りでした。Verizon の 2023 年データブリーチ調査レポートによれば、雑多なエラーに起因する 602 件の確認されたセキュリティインシデントのうち、23% は公開エラー（「誤った対象に何かを表示する」）によるものであり、21% は設定ミスによるものでした。IBM のデータブリーチのコストに関するレポート によれば、クラウドの誤構成は「攻撃の初期ベクトルとなるもので 11%」あり、それらの侵害の平均コストは 400 万ドルでした。

これは望まれる費用ではなく、それがなぜ私たちは 2024 年により多くの組織がクラウドインフラストラクチャ権限管理（CIEM）を優先し、最も安全なクラウド環境を提供できるベンダーに注力すると予想している理由です。クラウド環境を統合することで、組織はベンダーから二次的なリスクを引き継ぎます。第三者がエンタイトルメント、ツール、インサイダーの脅威をどのように管理するかは、顧客自体とそのデータに影響を与えます。規制された医療や金融サービスの組織では、患者や金融データの直接の所有権を失うことが、リスクを大幅に拡大させます。

中小企業がCIAMを実装する時期

クラウドサービスは、組織がインフラの変更するたびに、攻撃を拡大させ、新たなリスクを取り込みます。

顧客、契約業者、および第三者ユーザーは、組織の攻撃面を下から上へと拡大させます。組織が成長すると、より多くのユーザーがいて、それらの情報を管理する必要があります。その情報はさらに、GDPR や CCPA などのコンプライアンスの要件によって規制される可能性があります。規制されていなくても、顧客の情報を失うことは決して良い状態ではありません。

これが、私たちがより多くの組織が顧客アイデンティティおよびアクセス管理（CIAM）の機能を実装することを提言している理由です。これにより、ユーザーに関連するアイデンティティ制御を顧客、契約業者、労働者などに拡張できます。顧客に対して単なる認証以上のものを提供すると述べたように、組織は第三者ユーザーのアイデンティティを管理するためにガバナンス＆ライフサイクル、およびアクセスの機能を提供する必要があります。

重要なのは、IAM または CIAM を強調する必要があるのは大企業だけでないということです。サイバー犯罪者は Fortune 500 企業と小規模事業者の区別をつけません。情報がクラウド上またはオンプレミスで利用され、保持され、格納されていれば、組織の規模は重要ではありません。同じ要件が依然として適用されます。
変わるのは、その仕事を処理するために必要な人数と、特定のセキュリティインシデントがもたらす影響です。

これらが中小企業（SMB）から CIAM へのますます高まる関心を促進しています。実際、今年における SMB 向けのセキュリティにつながる行動を考えると、Verizon は「アクセスコントロール管理」をそのインシデントのコントロールの 1 つとしてあげています。

これらの機能は、「アクセスの資格情報と特権を作成、割り当て、管理、および取り消すためのプロセスとツール」の使用を含むべきであり、幅広いユーザー、管理者、およびサービスアカウントに拡張すべきです。

より多くのデータ、よりスマートな意思決定

テレビの中での話では、捜査官が画像にズームインし、「コンピュータ、拡大」と言うと、画像がさらに鮮明になるというものです。これをグラフィックデザイナーと一緒に見ると、大きく意見が食い違うかもしれません。（AI が写真や画像の解像度を増加させるだけでなく、他の便利なトリックもできるようになることを除いて）画像は最高の解像度から始めて、縮小する必要があります。専門家は、スケールでよりクリアな画像を得るには、魔法や特殊効果で情報を生成するのではなく、より多くの情報から始める必要があることを知っています。

> “中小企業（SMB）と大企業の両方が、類似したサービスとインフラストラクチャを使用しており、これは彼らの攻撃面が以前よりも共通するものが多いことを意味しています。これにより、組織のサイズに関係なく攻撃プロファイルが似たものになりました。ただし、大きく異なるのは、攻撃に対処するための組織のリソースの数によるもので、攻撃された場合に展開できる資源の数です”
>
> Verizon 2023 Data Breach Investigations Report

良いニュースは、上記で述べたトレンド、つまりクラウドでより多くの情報が結合し、さらに細かい情報をもたらすユーザーが増え、組織がクラウドで情報を統合する組織が増えると、組織が任意のユーザー、機械、サービス、またはその他のエンティティのより鮮明で明確なイメージを構築するためのデータを提供できるようになるでしょう。

より多くのディレクトリ情報と連携データおよび属性を活用することで、特定のリソースへのアクセスが必要な人物をより的確に特定できる広範囲のデータを得ることができます。この増加する情報量は、組織にははるかに高度なインテリジェンス、ダッシュボード、より良い判断と自動化を提供します。より多くの属性を持つことで、組織はより優れた、より制限の厳しいポリシーを設定し、ゼロトラストに一層近づくことができるでしょう。

“サイバーセキュリティで
AI が必要になっても、
人間のオペレーターは
消えない .”

AI は諸刃の剣。2024 年は、より深く切り込む.

メディアを見ていると、2023 年は AI 関連の情報に触れることが増えたかもしれません。AI は、司法試験に合格 することから『ミッション：インポッシブル』でイーサン・ハントと対決するまで、ほぼどこにでも存在していました。（ネタバレ注意）

AI については多くの期待があります。しかし、これは新しいリスクと新しいサイバーセキュリティツールの両方の可能性があるものです。2023 年には、研究者や攻撃者が AI を使用してポリモーフィック型 マルウェアを書き、トム・ハンクスが歯科保険を宣伝するディープフェイク広告を制作し、 フィッシングメールが 1,265% 増加しました。Verizon の 2023 年モバイルセキュリティインデックスホワイトペーパー によれば、「7 つの単語がサンプルとしてあれば、個人の声を信じられるレベルに偽装に作り上げるのに十分である」と報告しています。AI がより多くかつ説得力のあるフィッシング誘導、ディープフェイク、および他のソーシャルエンジニアリング攻撃を生み出す中、組織は自己を守るために強力な MFA を利用する必要があります。

AI が増加するリスクを表している一方で、AI は組織のサイバーセキュリティの態勢を向上させる上で重要なものとなります。 2023 年の RSA ID IQ レポート によれば、91% が AI がアイデンティティセキュリティの向上に役立つと考えており、実際、人々はセキュリティとプライバシーに関して技術を信頼しています。64% が、パートナーや親友、または金融アドバイザーではなく、情報を保護するためにコンピュータやパスワードマネージャーに信頼を寄せると回答しています。

Identity Defined Security Alliance の「2023 年のデジタルアイデンティティのセキュリティトレンド」調査によれば、アイデンティティおよびセキュリティ関係者の 98% が、AI と機械学習が有益であると考えていると考えています。

これらの認識は、AI への重要な投資に影響を与えています。Forrester Research によれば、2024 年までに AI ソフトウェア市場は 640 億ドル拡大し、その投資の恩恵を受ける成長速度が最も速い産業の一つがサイバーセキュリティです。

AI は検出を加速し、侵害の財務的なコストを削減し、組織全体のサイバーセキュリティの姿勢を向上させるのに役立ちます。 IBM Security の「データ侵害のコストレポート 2023」によれば、セキュリティ AI と自動化を使用する組織は、「データ侵害を特定および封じ込めるまでの時間が平均で 108 日短縮された」とされています。時間の節約は同時に費用の節約にもつながります。洗練された AI と自動化を採用する組織は、「データ侵害コストが平均で 176 万米ドル低減した」と報告しています。

人と機械–人VS機械ではない

サイバーセキュリティにおいて AI が必要であるからと言って、人間のオペレーターがなくなるわけではありません。それどころか、サイバーセキュリティの脅威に対抗するためには人間の専門知識が引き続き必要とされます。ただし、人間が行う具体的な仕事や AI との相互作用の方法は変わるでしょう。

近い将来では、AI が日常の業務を管理し、新規ユーザーのアカウントプロビジョニングを自動化し、ユーザーが MFA を有効にしていることを確認し、アカウントの異常を監視すると期待されています。AI がルーチン業務を管理する一方で、専任者はユーザーが他のメンバーが必要としないリソースを必要とする場合や、MFA の無効化などの高リスクな要求に対応する際など、より高度で影響力のある選択を監督します。

さらに AI は組織のサイバーセキュリティアーキテクチャの中核的な一部となり、そして、脅威者は組織のセキュリティ機能を回避しようと、プロンプト爆撃や MFA 攻撃と同様に、AI を標的にするようになるでしょう。AI に対する攻撃は、データ汚染やプロンプトの不正挿入、または AI を惑わせるように操り、新たな方法になるでしょう。

これはつまり、AI が私たちを守る一方で、私たちは AI を守る必要があるということです。

“2024 年に注意を
払うべき新興の
ランサムウェアリスクの
1 つは、BYOD です .”

もし今ラムサムウェア攻撃が悪いと思う？2024年はどうなる .

「もし壊れていなければ修理するな」というのは全ての人に当てはまります – これには悪い人も含まれています。2024 年においてもランサムウェアは彼らにとって有用なツールのままであり、依然としてトレンドとなり、コストを引き上げ続けるでしょう。 .

Verizon の 2023 年データ侵害調査レポートによれば、データ侵害の 24% がランサムウェアに関与しており、「ランサムウェアはあらゆる規模と業界の組織に普及している」と報告されました。Microsoft の Digital Defense Report 2023 によれば、「昨年と比較してランサムウェア攻撃の増加率が高まっており」、人間によるランサムウェア攻撃は「2022 年 9 月以来 200% 以上増加している」と報告されています。

理由はランサムウェアが儲かるからです。2022 年の FBI Internet Crime Complaint Center (IC3) によれば、被害者がランサムを支払った事件の中で、中央値の損失は 1 年間で倍以上に増加し、26,000 ドルになり、95% のケースでの損失範囲は 100 万ドルから 225 万ドルでした。IBM Security の「データ侵害のコストレポート 2023」によれば、ランサムウェア攻撃の平均コストは「前年比で 13% 増加」し、平均コストは 513 万ドルになりました。

2023 年の ALPHV ランサムウェア攻撃が 2023 年のコストを引き上げると予想されます。シーザーズ・エンターテインメントは報道によれば 1,500 万ドル支払い、MGM リゾーツ・インターナショナルは侵害の結果として 1 億ドル の費用を予測していました。ランサムウェアが増加しており、そのような重大な財務的影響をもたらす可能性があるため、組織は安全を維持するために強力な MFA および他のサイバーセキュリティ対策を実施する必要があります。

2024 年に注視すべき新興のランサムウェアリスクの一つは？それは「Bring Your Own Device (BYOD)」です。Microsoft によれば、「すべての成功したランサムウェアの侵害の 80% -90%は、管理されていないデバイスを介して起こる」という結果があり、「通常、管理されたハードウェアよりもセキュリティコントロールと防御が少ない」とされています。

ランサムウェアの数値による分析：

513万ドル

ランサムウェア攻撃対策にかかる平均コスト

13%

2022 年から 2023 年までのランサムウェア攻撃の平均コストは年々増加

100万ドル

MGM Resorts International による ALPHV 2023 ランサムウェア攻撃の予想されるコスト

2022 年 9 月以来、人間による操作のランサムウェア攻撃が 200%増加 しました .

MFA: 良いニュースと悪いニュース.

良いニュースは、MFA を要求する規制がサイバーセキュリティのレベルを高く維持するのに役立つでしょう。イギリスでは、国民保健サービス（NHS）が 2024 年 6 月 までに MFA を導入する要件出され、医療および患者データを保護するのに役立ちます。また、ヨーロッパ連合は 2024 年 10 月までに加盟国に対して Network and Information Security 指令（NIS2）の適用を開始するよう要求し、「場合に応じた適切な多要素認証の使用」を含んでいます。米国では、バイデン政権の「国家のサイバーセキュリティを向上させるための大統領令」により、すべての連邦民間行政機関は 2022 年に MFA の実施を開始する必要がありました。

悪いニュースは、MFA がサイバーセキュリティに不可欠である一方で、過去数年の最悪のデータ侵害の中には、MFA だけでは不十分であることを示したものもあります。

新しい AI 脅威、ランサムウェア、そして増加する攻撃は、組織が MFA を最初の防衛ラインとして優先する緊急性を強調しています。**サイバーセキュリティは認証から始まる**

MFA: 良いニュースと悪いニュース.

タイムライン

2022 年 3 月

ロシアの脅威者は、新しいデバイスを MFA に登録することで、非政府組織に侵入しました。その後、「 デフォルトの MFA プロトコルに設定された誤構成アカウントを利用しました」と述べ、インターネットから切断することで MFA をバイパスすることができました

LAPSUS$ ハッキンググループは、Okta のサードパーティの顧客サービスプロバイダーを侵害し、そのアクセスを利用して「テナント管理者グループ」に新しいアカウントを追加し 366 人の顧客を侵害しました。

2022 年 9 月

Uber の従業員の Active Directory パスワードを入手した後、攻撃者は Uber の IT をなりすまし、MFA の攻撃 を使用してユーザーに MFA プロンプトを洪水のように送り、リクエストを承認するまでにアクセスを提供しました。これにより、Uber のバグバウンティプログラムにアクセスできるようになりました。

2022 年 11 月

攻撃者は、MFA に登録したユーザーに発行された クラウドトークンを盗み出しました。その後、盗まれたトークンを使用して、異なるデバイスからアクセスを得ました。

2023 年 6 月

Microsoft は、2023 年 6 月末までに 1 日あたり約 6,000 回の MFA 攻撃を計測しました。

2023 年 8 月

Microsoft 365 を標的としたキャンペーンでは、EvilProxy が使用されました。EvilProxy は、「逆プロキシの戦術を使用して MFA をバイパスする」フィッシングツールキットで、上級幹部が犠牲になるほどの成功を収めました

2023 年 9 月

Caesars Entertainment、MGM、および他の組織は、脅威アクターが顧客サービスデスクをフィッシングした後、攻撃者が Okta のスーパーアドミンアカウントへのアクセスを許可するために MFA をリセットできるようになったことにより、侵害されました。

2023 年 10 月

BeyondTrust and CloudFlare は、自社のアイデンティティインフラストラクチャに対する攻撃を発見しました。攻撃は、攻撃者が Okta のサポートデスクと HAR ファイル にアクセスしたことの一部から起こりました。

The Citrix Bleed 脆弱性は、攻撃者にパスワードと MFA の要件をバイパスする手段を提供しました

MFA は重要なサイバーセキュリティの構成要素であり、政府やビジネスが MFA を実施するために行ってきた作業のため、2024 年においても攻撃者は MFA を迂回する方法を模索し続けるでしょう。さらに、成功した攻撃は組織のアイデンティティインフラの隙間を悪用すると予想されます。

MFA は最初の防衛ラインであり、最後の防衛ラインではない.

「資格情報を盗む方法はたくさんありますが、それを保護する方法もたくさんあります。その中でも最も優れた方法の一つ（これまでに聞いたことがあれば止めてください）は MFA の使用です。椅子に寄りかかって「まあ、実際には ...」と言われる前に、私たちはいくつかの MFA 実装には制限があることを理解しています。おそらくご存知の通り、今年のいくつかの非常に高いプロファイルの侵害事件は、それらの欠点の一部を示しています。」

いくつかのケースでは、犯罪者はソーシャルエンジニアリングを使用してユーザーを説得し、認証試行を受け入れさせました。別のケースでは、彼らはセッションクッキーを盗み、それを使用してユーザーのふりをしていました。もちろん、一部の MFA 回避は実際には MFA をバイパスしていなかったのは、一部のサービスが適切に構成されていなかったため、「MFA のみを使用する」ように設定されていなかったからです。

Verizon 2023 データ侵害調査レポート：

“ 安全の錯覚”

「MFA はセキュリティの向上を助けるためのものです。しかし、私たちは以前のレポートで議論したように、それは万能薬ではありません。実際、MFA を導入することで生じる安全の錯覚そのものがリスクです。」

ますます、SMS や認証アプリを基にした MFA の種類は取って代わられつつあります。多くのアプリケーションは、ユーザーに対してモバイルデバイス上のアラートに対する応答（通常は受け入れまたは拒否）を求める形式の MFA を使用しています。

MFA スパム攻撃では、攻撃者はユーザーに対して確認のプロンプトを大量に送りつけ、その人が「受け入れ」をクリックして迷惑を取り除いてしまうことを期待しています。実際にそれを行う人もいます。

2022 年、Uber は MFA 攻撃に起因する高いプロファイルの侵害に見舞われました。攻撃者は、請負業者の侵害された VPN 資格情報を使用して繰り返しログインを試みました。これが成功しなかったとき、攻撃者は WhatsApp で被害者に連絡し、Uber IT サポートを装い、従業員にリクエストを受け入れるように促しました。そして、従業員は受け入れました。攻撃者は VPN へのアクセスを悪用して、企業のメール、クラウドストレージ、コードリポジトリなどの重要なシステムに侵入しました。

2023 年モバイルセキュリティインデックスホワイトペーパー

サービスデスクはユーザーのためのライフラインであり、攻撃者のための標的になってはならない。

数年にわたり、脅威者は IT や組織のヘルプデスクをなりすまして、ソーシャルエンジニアリングを行ってきました（Uber を侵害した攻撃者は、企業の テクニカルサポート チームの一部として装った）

しかし最近、攻撃者は標的を変更し、ヘルプデスク自体を攻撃 しています。その理由は明らかです。ヘルプデスクはアカウントを作成したり、MFA を一時停止したり、パスワードをリセットしたりする広範な権限を持っており、これは攻撃者自体が行いたいこととほぼ同じです。さらに、彼らは VIP から「緊急」なリクエストを受けることに慣れています。そして、組織はユーザーや従業員が接続し、生産的でいることを望んでいるため、ヘルプデスクの連絡先情報はオンラインで簡単に見つけることができます。

これらの要因はすべて、ヘルプデスクを魅力的で、かつ収益性の高い標的にします。MGM は、脅威者がカスタマーサービスデスクをフィッシングし、攻撃者が MFA をリセットできるようにしたことから始まったランサムウェア攻撃により、約 1 億ドル の損失を受けました。シーザーズは、システムを復旧するために攻撃者に報告された 1,500 万ドル を支払いました。サポートシステムは、将来の攻撃に使用される可能性のある、ユーザーに関する膨大な情報を収集します。 2023 年 10 月の侵害 により、脅威行為者はサポートシステムのユーザーのすべての名前とメールアドレスをダウンロードすることができました。これは、「フィッシングやソーシャルエンジニアリング攻撃のリスクが増加する可能性があります」。

組織は、ヘルプデスクが被害を引き起こさないために、以下のことをする必要があります：

- **理解**：ヘルプデスクがどのような行動ができ、どのようなアクセス権を持っているかを理解する
- **文書化**：実行手順書やプロセス、ルプデスクが他のグループを巻き込むケースを文書化する
- **確立**：変更管理プロセスに従う必要がある高リスクなアクションを確立する
- **創る**：年次のコンプライアンストレーニングを導入するだけでなく、セキュリティが最優先事項であるというリーダーシップが一貫して伝えられるセキュリティファーストの文化を創る
- **実践**：リーダーシップを持ってヘルプデスクが規定に従って行動した場合に支援することを示す
- **統合**：オンボーディング時に資格情報のブートストラップを行うために身元確認を統合する

最後のポイントは、ハイブリッドワークが産業全体に定着するにつれて特に重要になります。5 年前と比べて、オンボーディングは直接対面で行われる頻度が低くなる可能性があります。これは、認証が初期登録に依存する限り、サイバーセキュリティにとって重要な変化を表しています。組織は、新しいアイデンティティの強力な防御を確立するために、より広範な身元確認の機能が必要になります。

防御から自己防衛へ

アイデンティティは常に防衛者の盾でありました：アカウントの作成、認証の確立、および権限の設定は、組織がリソースを認識し、管理し、保護する必要性から生じます。

しかし、もしアイデンティティが組織の盾であるなら、それは同時に攻撃者の標的でもあります。これは必ずしも新しい問題ではありませんが、例年の Verizon Data Breach Investigations Report を見ても、おそらくその年の主要な初期攻撃ベクトルの 1 つがアイデンティティであったことがわかるでしょう。しかし、それが新しい問題ではなくても、成長するセキュリティの脆弱性としてのアイデンティティは、さらに悪化する可能性があります。増加するユーザー数、デバイス数、権限、環境が、より大きく、より複雑で、より脆弱なアイデンティティ攻撃面を形成しています。昨年のデータ侵害では、攻撃者がこの成長を自分たちの利益に活用しました。

アイデンティティが防御に優れているだけでは十分ではありません－それは自己防衛にも優れる必要があります。 アイデンティティ脅威検知と対応（ITDR）は、アイデンティティを単なる強力な盾以上にすることができる新しい機能です。これによりアイデンティティは、積極的に脅威を検知し、防御することも含むことができます。

私たちの免疫系に最新のブースターが必要であることは明らかです。人間は何十万ものイベントから生じるログを解析して異常を見つけることはできず、静的なルールセットは思考する敵に対応するには適応力が不足しています。しかし、AI はできます – 実際、人間とは異なり、AI はより多くのデータを与えると改善します。

セキュリティに関してすべての AI が同じように作成されるわけではありません。 決定論的 AI は、セキュリティと監査チームがコンプライアンスを維持し、セキュリティオペレーションを自動化するために必要な透明性を提供する傾向があります。AI は特に以下の点が優れています：

1. **認証データ**：誰が入ろうとしているかを理解するためのデータ
2. **アカウントと権限情報**：誰かがアクセスできる可能性があるものを理解するための情報
3. **使用データ**：実際に何をしているかを見るためのデータ

機械の台頭

人間のユーザーだけではありません：サイバーセキュリティは、ログインする実際の人間に加えて、機械、インターネット・オブ・シングス（IoT）、およびサービスアカウントも考慮する必要があります。そして、これをアイデンティティライフサイクルの各段階で行わなければなりません。
2023 年、あるハッキンググループが、ベンダーとその 顧客間で送信されるパスワードを見つけるために API を使用しました。攻撃者は API を使用してバックドアサービスアカウントを作成しようとし、実際はできませんでしたが、その機会を与えるべきではありませんでした：初期の API 交換、つまり 1 つのサービスアカウントが別のアカウントに情報を送信することは、リスクがあります。これらのサービスアカウントが何を送信しているかについての監視が限られていたため、このリスクが悪化しました。サービスアカウントでさえ、クリアテキストのパスワードを送信すべきではありませんし、どのパスワードも、それが動作している機器に特定されるべきです。同様のリスクが Colonial Pipeline, でも発生し、非アクティブな VPN アカウントが MFA で保護されていなかったため、そのエネルギー提供者に対するランサムウェア攻撃の発端となりました。
そのリスクは拡大する可能性があります。2022 年には、IOT に接続されたデバイスの数が 18%増加し、143 億台に達し、今年はさらに 16%増加して 167 億台 に達すると予想されています。これは非ユーザーベースのアカウントが情報を交換する多くの機会です - そして、サイバーセキュリティチームがカバーする必要がある範囲もさらに広がります。

“法律と
専門サービスは、
リスクが増大 .”

法律業界と専門コンサルティングは攻撃の標的に.

米国には、化学、通信、エネルギー、金融サービスなど、16 の重要インフラセクターがあります。米国サイバーセキュリティインフラストラクチャ＆セキュリティエージェンシー（CISA）は、これらのセクターを「米国にとって極めて重要であり、その機能停止または破壊が安全保障、国家経済安全保障、国民の公衆衛生または安全、またはそれらの組み合わせに深刻な影響を及ぼす可能性がある」と定義しています。

多くのサイバーセキュリティ要件は、これらの 16 のセクターとそれらの内部で活動する組織に焦点を当てており、これらの要件は重要インフラのより高いサイバーセキュリティ基準を作成するのに役立ちました。さらに、2024 年までに連邦民間機関がある程度のゼロトラストアーキテクチャを採用するという期限は、エネルギー、交通などの重要なインフラが多くの攻撃に耐えるようになることを意味し、攻撃者は他のより脆弱なターゲットを探すことになるでしょう。

我々は、敵対者がサイバーセキュリティ要件の不足しているセクターに焦点を当てると予想しています。特に法律事務所や専門コンサルティング企業です。これらの業界はリスクの完璧な渦を表しています：彼らは特権のある機密情報を取引していますが、サイバーセキュリティ対策が万全とは言い切れません。

“.... モバイルデバイスは
不可欠なツール。
企業の主要システム、データ、
およびクラウドベースの
リソースへの重要な
エントリーポイントとして機能。
しかし、リソースをリスクに
さらす可能性が増大 .”

2024 年、組織はモバイルセキュリティの問題に対応する新たな方法を探す.

2022 年末までに、54 億以上 の人々が携帯サービスに加入し、44 億人が携帯デバイスからインターネットにアクセスしました。モバイルアプリは 2022 年に 4000 億ドルの収益を生み出しました。

驚くべきことに、電話はユーザーがより安全に保つのに役立つこともあります：それらは MFA での ID 証明として機能する「何かを持っている」と「何かである」という要素を満たします。2023 年末までに、86%の人々が電話を主要な認証器として使用していました。（73% がスマートフォンは最も便利な MFA 方法だと考えていました）これにより、データ侵害の大部分に関与しているパスワードを排除するのに役立ちます。

しかし、すべてのサイバーセキュリティの可能性があるにもかかわらず、電話や他のデバイスは完璧なセキュリティの黄金時代をもたらしていません。脅威者は我々が良いものを持つことを許しません：2021 年から 2022 年にかけて、モバイルマルウェアのサンプルは前年比 51% 増加しました。
マイクロソフトは、ランサムウェアのターゲットとなるパターンを詳細に説明する中で、「すべての侵害の 80 ～ 90%が管理されていないデバイスから発生する」と述べられています。フォレスター によると、従業員所有のモバイルデバイスは、IOT デバイスに続いて、外部攻撃の 2 番目に一般的な標的でした。

MFA の潜在能力にもかかわらず、ユーザーの電話は重大なリスクを招きます。 2023 年の RSA ID IQ の回答者の約 3 分の 2（72%）が、人々がしばしば個人のデバイスを専門的なリソースにアクセスすると信じていました。同じ調査では、ほぼすべての（97%）サイバーセキュリティ専門家が、ユーザーの電話が重要なサイバーセキュリティリスクを表すと信じていました。なぜなら、ユーザーが：

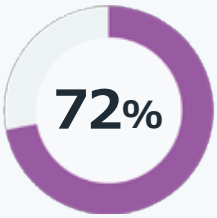
- デスクトップよりもモバイルデバイスでの**電子メールの開封が多かった**
- モバイルデバイスでの電子メールの**検証がより難しかった**
- 個人のデバイスから**専門リソースにアクセスした**

個人のデバイスは管理されたデバイスよりもセキュリティコントロールが少ない傾向があるという事実を加えると、モバイル電話が攻撃面を拡大していることが明確です。

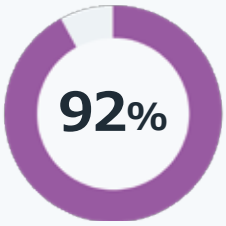
他のリスクとは異なり、企業は自前のデバイス（BYOD）ポリシーを逆戻りするつもりはありません。2023 年の Samsung の 報告書 によると、全従業員にモバイルデバイスを支給している企業はわずか 15%に過ぎません。昨年、Zimperium は、企業資産にアクセスするエンドポイントの 60%がモバイルデバイス上にあることを発見しました。そのため、一部の報道機関が 2015 年以来、BYOD を「根強い」と呼んでいるのも不思議ではありません。

組織はどうすればよいのでしょうか？雇用主は、個人のデバイスにセキュリティや監視ソフトウェアをインストールすることを要求することはできません。しかし、組織内での個人デバイスの使用に伴う固有のセキュリティ上の弱点を制御および維持する方法が必要です。
このため、私たちは 2024 年に、組織がユーザーの個人の電話に関してセキュリティと利便性の両方をバランスさせる方法に焦点を当てると予測しています。ユーザーが電話を認証器として使用する場合、ユーザーの個人のデバイスに複数のアプリやダウンロードを課すことなく、認証プロセス自体を保護する解決策を提案しました。

2023 年 RSA ID IQ レポートは、モバイルデバイスのリスクを強調：



72%の回答者が、人々が頻繁に個人のデバイスを使用して専門のリソースにアクセスしている



92%のサイバーセキュリティの専門家が、ユーザーの携帯電話が重要なサイバーセキュリティリスクと考えている

"…モバイルデバイスは不可欠なツールとなっています。これらは、企業の主要システム、データ、およびクラウドベースのリソースへの重要なエントリーポイントとして機能します。同時に、これらのリソースを危険にさらすこともあります。

モバイルデバイスは生産性と柔軟性の大幅な向上を提供しますが、同時に数多くのセキュリティ上の課題をもたらします。堅牢なセキュリティ、生産性、コストのバランスをとることは簡単ではありません。さらに、組織はユーザーエクスペリエンスとプライバシーも考慮する必要があります。

ユーザーに過剰なセキュリティ対策を課すことは生産性を減退させる可能性があります。しかし、緩いセキュリティプロトコルは重要な企業システムや資産を脅威にさらす可能性があります。このバランスを正しくとることは、キャリアに影響を与える、将来を決定する、取締役会レベルの問題です。

モバイルデバイスを効果的に保護し、それが組織のアキレス腱になることを防ぐには、堅牢なセキュリティを提供しつつ、シームレスなユーザーエクスペリエンスを確保するソリューションを活用することが必要です。"

Verizon 2023 Mobile Security Index のホワイトペーパー

RSA であなたのアイデンティティの未来を安全に保護.

RSA ID Plus の無料トライアルにサインアップして、私たちがどのようにあなたの組織を安全に保護できるかを直接体験してください。新しい脅威に適応したり、AI の力を活用したり、MFA を導入したり、アイデンティティセキュリティ機能の完全なコンポーネントを開発したりする場合、RSA は 2024 年に検討を進めているあなたの組織に対するソリューションがございます。新しい方法で安全に接続され、生産的であるためのものをお探しであれば、RSA がお手伝いいたします。

ID Plus の無料 45 日間トライアルを開始

RSAについて

AI 搭載の RSA Unified Identity Platform は、世界で最も安全な組織を今日と明日の最も高リスクのサイバー攻撃から保護します。RSA は、脅威を防ぎ、アクセスを保護し、コンプライアンスを可能にするために必要なアイデンティティインテリジェンス、認証、アクセス、ガバナンス＆ライフサイクルの機能を提供します。9,000 以上のセキュリティ第一の組織が、オンプレミス、ハイブリッド、マルチクラウド環境全体で 6,000 万以上のアイデンティティを管理するために RSA を信頼しています。詳細は、RSA.com で