CISO向け エンタープライズ ソフトウェア セキュリティの 未来に関するガイド

Rimini Street®

サイバー・セキュリティの脅威がより頻繁かつ高度になるにつれ、最高情報セキュリティ責任者（CISO）は、自社のエンタープライズ・アプリケーションが格好の標的であることを痛感しています。最近発表された「CISOの声」というタイトルのレポートでは、CISO の半数が、自分の組織が今年、重大なサイバー攻撃の標的になる可能性があると報告しています。[1]

自然災害による絶え間ないリスクと、サイバー攻撃と対策の高度化により、セキュリティ専門家はスキルアップに奔走し、その結果、サイバーセキュリティは2022年に、IT で不足しているスキルリストのトップにランクインしました。構築可能なインフラストラクチャの普及が進んでいること、現実のリモートワークの性質、クラウドベースのソリューションへの依存の複雑さを考えると、エンタープライズアプリケーションのセキュリティ保護の競争が近いうちに弱まることはありません。[2]

しかし、社内のスタッフでアプリケーションのセキュリティを一から構築するには、深い専門知識と技術を必要とし、組織のリソースと予算を圧迫する可能性があります。ベンダーのパッチのみに依存することは、堅牢なセキュリティ戦略にはほど遠いものです。そして、ほとんどの人にとっては受け入れがたいレベルのリスクも伴います。しかし、内部スタッフを使ってゼロからアプリケーションの堅牢なセキュリティを構築するには、深い専門知識と、組織のリソースと予算を圧迫しかねないテクノロジーの使用が必要になります。

ベンダーのパッチのみに依存することは、堅牢なセキュリティ戦略にはほど遠いものです。

しかし、社内スタッフを使ってアプリケーションの堅牢なセキュリティを構築するには、深い専門知識と、組織のリソースと予算を圧迫しかねないテクノロジーの使用が必要になります。

ベストプラクティスのアプローチを活用し、よりリスクの高いリソースや価値の高いリソースをモダナイゼーションの取り組みに集中させ、サイバーに精通した人材を育成することは、多くの企業にとって重要な課題となっています。 これを実現するために、多くの組織が信頼できるパートナーに監視、対応、テクノロジーの導入といった作業を依頼しています。

サイバー・セキュリティへのベスト・プラクティス・アプローチ

強力なサイバー・セキュリティ体制を構築するには、ベストプラクティスに沿う必要があります。
現在では、セキュリティに対するゼロ・トラスト・アプローチとサイバー・セキュリティ・メッシュ・アーキテクチャ・アプローチの両方が採用されつつあります。この2つのアプローチにはそれぞれ異なる重点分野があり、エンタープライズ・アプリケーションのセキュリティを含むサイバーセキュリティのあらゆる側面において有効です。また、この2つのアプローチは補完的なものでもあるため、両方を採用することで優れた結果を得ることができます。

サプライチェーン・セキュリティ

Log4Jの登場とSolarWindsのアップデート進行による伝播は、デジタル・サプライチェーンに関連するリスクとそのセキュリティ確保の必要性を露呈しました。CISOは、ベンダーが最低限の要件を満たしていることを確認するための標準とポリシーを導入する必要があります。ソフトウェアやアプリケーションの場合、ベンダーは、リリース前にデジタル資産の脆弱性をテストし、安全性を確保するために、安全なソフトウェア開発ライフサイクル（SSDLC）プロセスを確立し、それに従わなければならないことになります。

さらに、サプライチェーンセキュリティ計画の一環として、ベンダーは、パッチ・プログラムが存在し、かつ、発見された脆弱性に対してはタイムリーにパッチをリリースすることを確認する責任を負わなければなりません。ソフトウェア・ベンダーは、パッチを重大な脆弱性のみに限定するのではなく、顧客に実質上のリスクをもたらす、あらゆる脆弱性に適用する必要があります。

ゼロ・トラスト・アプローチ

従来の境界型セキュリティでは、企業のファイアウォールが、信頼できない人々を企業ネットワークの外に出し、重要な資産から遠ざけていました。通常、ユーザーにはまとまったレベルの権限が与えられ、必要でないリソースにもアクセスできるようになります。これは、タスクの実行に必要最小限の権限をユーザーに付与すべきという、最小権限アクセスの概念に違反しています。

認証が成功したときに付与される権限によっては、ユーザーは実質信頼できる存在と見なされるため、ファイア・ウォールやその他のセキュリティ制御を通過できる場合があります。この環境では、悪意のある人物が（フィッシングや類似の活動を通じて）正規のログイン認証情報を取得した場合、重要な企業リソースやデータへの不正アクセスができてしまう可能性があります。

「ゼロトラストは考え方であり、特定のテクノロジーやアーキテクチャではありません。絶対的な信頼をゼロにするという考え方です。絶対的な信頼というものは、あってはなりませんから」

– ニール・マクドナルド氏
Gartner VP特別アナリスト[3]

悪意のある人物がファイアウォールの内部に入ると、既知の脆弱性を利用してエンタープライズ・アプリケーションを侵害する、バックドアをインストールして機密データを盗み出すなどの操作を実行する可能性があります。同様に、特定のアプリケーションに害を及ぼすことが知られているウイルスを導入する可能性もあります。こうしたリスクを軽減するために、組織は既知の脆弱性に対するセキュリティパッチを提供するアプリケーション・ベンダーに依存してきました。

セキュリティは、アプリケーションに定期的にパッチを適用することで強化できます。しかし、セキュリティパッチは、予期せぬアプリケーション障害を招く可能性があります。定期的、またはタイムリーにパッチを適用するリソースが不足しているため、多くの場合、遅延が発生していました。

1つの鍵で開く入口は1つだけです。

サイバー・セキュリティのゼロ・トラスト・アプローチは、デフォルトで全ての組織とリソースを信頼できないものと見なします。例えば、有効なネットワーク・ログイン認証情報を持っていれば、ネットワークの指定された領域へのアクセスが許可されますが、ネットワークのその部分内のリソースを使用したり、データにアクセスするには、更なる認証が必要になります。1つの鍵でネットワーク内の領域には入れますが、その中では、全てのデータが個別に施錠され、アクセスできないようになっています。

ゼロ・トラスト・アプローチは、悪意ある者が1組の認証情報やネットワークの一ヵ所への侵害によって引き起こし得る損害を制限するものです。また、まだパッチ未適用のエンタープライズ・アプリケーションへの脅威も軽減します。

サイバー・セキュリティ・メッシュ・アーキテクチャ・アプローチ (CSMA)

ゼロ・トラストがアイデンティティ、アクセス、信頼の問題に焦点を当てているのに対し、サイバーセキュリティ・メッシュアーキテクチャ（CSMA）アプローチは、セキュリティツールやソリューションの共同エコシステムを構築することを目的としています。これらのツールは、相乗的に連携し、従来の境界線を遥かに超えてセキュリティを拡張できるものです。

CSMAの原理では、サイバーセキュリティはテクノロジーだけに当てはまるものではないと認識されています。プロセスや人が重要です。そのため、CSMAアプローチは、セキュリティと、ビジネスプロセスの両方が確実に準拠することが求められます。

サイバー・セキュリティ・メッシュ・アーキテクチャの要素

CSMAがどのように形成されているかを理解するためには、アーキテクチャを構成要素に分解すると良いでしょう。サイバーセキュリティ・メッシュ・アーキテクチャの主要レイヤーは、ネットワーク・アーキテクチャとクラウド・アーキテクチャのいずれとも異なりますが、類似のアーキテクチャが存在します。

セキュリティ分析と脅威インテリジェンス

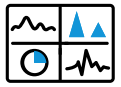
ここで重要なのはデータの一元化と分析であり、それには統合の問題を引き起こす可能性のあるソリューションからそのデータにアクセスする必要があります。

一元化されたポリシー管理と編成

オーケストレーションを実現する方法はさまざまですが、基本的な考え方は、ハードウェアやソフトウェアなど、あらゆる資産がオーケストレーションをサポートし、可能にすること、そしてサイロを回避することです。

アイデンティティ・ファブリック

CSMAでは、IDの強調はコンテクスト認識にあります。これはゼロ・トラスト・アプローチと一致するもので、人を超えてシステムやデバイスにまで及びます。



ダッシュボード

ここでも一元化が重要です。メッシュの概念は、全てのアセットとリソース間の相互接続性を示し、包括的なダッシュボードを可能にします。

CSMAが対処できる課題

サイバーセキュリティ・メッシュ・アーキテクチャを採用してセキュリティ・ツールを統合し、共同のエコシステムとして機能させることで、個々のセキュリティ事故の経済的影響を削減することができます。その場合の、2024年までの平均削減率は次の通りです。

90%

–ガートナー社[4]

CSMAが成熟するにつれて、今セキュリティ・チームが直面する最も困難な課題を対象とした、メリットや機能が提供されるようになっています。以下のような課題に対処できます。

- **境界の断片化**
  モバイル・デバイスの数や種類の増加、リモートワーカー、クラウドベースのアプリケーションなど、あらゆる要因が絡み合って、従来のセキュリティ境界は時代遅れになっています。
- **セキュリティ・サイロ**
  専門的なセキュリティツールは、特定のタスクを個別に効率的に実行し、報告します。これらのツールを管理するチームは、他の活動との間で調整したり、自動的にデータを共有する手段を持っていないことが多いです。
- **不十分なインテグレーション**
  ベストオブブリードのセキュリティソリューションの中から選択する場合、相互運用性がベストオブブリードの基準にはないことが多いことがすぐに分かります。
- **疲労困憊するセキュリティ部門**
  サイバー・セキュリティは、1日24時間稼働しています。データ侵害がもたらす結果は深刻です。セキュリティ技術は急速に進化するため、セキュリティ担当者は常に学習し続ける必要があります。担当者は、技術の先を行かなければならず、また深夜3時のシステムアラートの結果に対処しなければならない日々で、燃え尽きてしまうことがよくあります。
- **連係した対応**
  サイバー・セキュリティ・チームは、企業のアセットが危険にさらされている可能性があることを示すイベントや情報を検出して対応する必要があります。これらは、地震などの自然現象、またはサイバー攻撃やテロなどの人為的な出来事に関連している可能性があります。CSMAは、自動化技術、分析、人工知能を利用して、ネットワークとリソースを監視します。脅威を迅速に特定してサイバーチームに警告し、プレイブックを使って影響を最小限に抑えるなどの対策を講じます。
- **非効率的なセキュリティ運用**
  CSMAはセキュリティ組織、特に運用組織が最高の効率で機能するよう強制します。これは、破壊的、攻撃的な侵入者からの被害を最小限に抑え、ビジネスの継続性を維持するために必要なことです。常に一歩先を行くためには、セキュリティ運用チームは、SIEM（セキュリティ情報イベント管理）、分析、および関連インフラストラクチャなどの革新的なサイバーセキュリティプロセスとツールを必要とします。セキュリティをうまく運用するには、ツールやプロセスを管理するチームがCSMAを高度に使えるように訓練されていなければなりません。
- **リスクの増大**
  CSMAによって全体的な改善が図られるため、企業のセキュリティ態勢が強化され、全体的なリスクが低減されます。CSMAフレームワークを完全に実装している企業は、脆弱性や弱点をついたサイバー攻撃の影響を受けにくくなります。

セキュリティの近代化による技術的負債の削減

想定された寿命を超えて使用されているハードウェアとアプリケーションは、最新の装置ならクローズできている攻撃ベクトルを作ってしまう可能性があります。これは、時代遅れのハードウェアとアプリケーションでは、最新のセキュリティアプローチとテクノロジをサポートできない可能性があるためです。古いリソースでホストされている機密または重要な企業データとデータベースは、最もアクセスしやすい脆弱性を利用したバックドアなどの攻撃を受ける可能性があります。

ただし、古いハードウェアとアプリケーションのアップグレードは、費用がかかり、混乱を招く可能性があります。最初のステップは、従来のリソースがリスクを生み出しているかどうかを判断し、そのリスクの程度を評価することです。これには、ペネトレーション（侵入）テストや脆弱性スキャンなどの手順を使用して機器やアプリケーションを監査し、セキュリティホールをクローズする必要があるセキュリティホールを特定することが必要です。

データベースの堅牢化とセキュリティ保護は、データがどこに存在するかにかかわらず、攻撃対象領域を減らすのに役立ちます。これらの文書では、Oracleなどの特定のベンダーのデータベースを堅牢化するためのガイダンスと、多くのデータベース（DB2、MS SQL Server など）に適用できる最小限の許容ベースライン構成による、より一般的なガイダンスを提供しています。

デジタル市民の育成

CSMAについて、人がサイバーセキュリティの重要な構成要素であることを先ほど述べました。ほとんどの侵害の原因はヒューマンエラーです。このエラーにはいくつかの形があり、一般的なのは、定期的にパスワードを変更しない、複数の場所で同じパスワードを使用する、簡単すぎるパスワードを作成する、パスワードを共有するなどといった、認証情報の誤まった使い方です。

IT環境内部から発生するエラーもよくあります。ネットワーク、アプリケーション、デバイス、ファイアウォール、および他の形式のテクノロジーや設定ミスの可能性があります。その結果、通常では存在しない脆弱性が生じ、ひとたび悪用されれば、壊滅的な結果を招く可能性があります。これは、マルチテナントのクラウド環境において特に顕著です。

サイバーセキュリティの人的要素への取り組みは、教育から始まります。年次コンプライアンス研修以外でも研修を取り入れましょう。フィッシングテストなどの方法を使用して組織全体の従業員を教育することで、トレーニングの有効性を測定するためのベースラインデータを入手でき、従業員のセキュリティ意識も高まります。また、情報漏えいに関するニュースにも関心を寄せて、常にサイバーセキュリティを念頭に置きましょう。

82%

この数字は、2021 年に認証情報の盗用と悪用、フィッシング、または単純な人的ミスなど、人的要素が関与したデータ侵害の割合です。

– ベライゾン社[5]

人材戦略

先ほど述べたように、サイバーセキュリティのスキルは、IT人材採用ニーズの上位を占めています。社内のセキュリティチームの人材確保に関しては、現在のニーズに対応し、将来必要となるスキルを身につけることができるよう、多角的な戦略を立てる必要があります。

必要なスキルを理解したら、再訓練と再教育を通じて既存の人材を育成します。また、学校とパートナーシップを構築して、新しい才能を獲得することも検討してください。採用または再研修によって必要なスキルを獲得できない場合は、必要なセキュリティの専門知識を提供できることに加え、今後セキュリティ戦略展開を支援してくれる信頼できるセキュリティ管理サービスプロバイダー（MSSP）を探すと良いでしょう。

MSSPは、階層型セキュリティモデルに対応するサービスを提供することが可能であり、あらゆる規模の企業がコスト効率の高い方法で多重防御を実現できるよう支援します。信頼できるMSSPを利用すると、必要なサイバーセキュリティ人材が獲得でき、サイバーセキュリティと脅威の進化に合わせて改善できる、革新的で強力なサイバーセキュリティツールを入手できます。

「Oracleのセキュリティ・パッチは四半期ごとにリリースされます。多くの場合、最大で12か月前の脆弱性に対処するものであり、システムが 12 か月間脆弱であった可能性があることを意味します。最新のセキュリティ・アプローチを使用して、リミニストリートのアドバンスト・セキュリティ・ソリューションがシステムをより適切に保護してくれることが分かりました。このアプローチを採用することで、大学にとってより価値のある業務にリソースを充てることが可能になりました。」

—スコット・ローリー氏 クイーンズランド工科大学・ソリューション・デザイン&デリバリー部門・アソシエイト・ディレクター

注釈

1 Proofpoint. “2022 Voice of the CISO,” May 05, 2022
2 CXOtoday.com. “Most In-Demand Tech Skills for 2022 and Beyond,” January 09, 2022, Sohini Bagchi
3 Verizon. “2022 Data Breach Investigations Report,” June 03, 2022
4 Gartner, Inc. “New to Zero Trust Security? Start Here,” June 02, 2021, Susan Moore
5 U.S. Department of Defense. “Security Technical Implementation Guides (STIGs)”

まとめ

エンタープライズ・アプリケーションは、悪意のある人間にとって格好の標的であり、CISOの約半数が近いうちにサイバー攻撃を受けると予測しています。エンタープライズ・アプリケーションのベンダーにサイバーセキュリティを依存する場合、セキュリティ・チームはパッチが利用可能になったときに迅速に対応する必要があります。それでも、パッチは未知の脅威を防ぐことはできません。先進的なCISCOは、ベンダーのパッチを超えて、既知および未知の脆弱性から保護する階層的なセキュリティ・モデルを構築しています。層構造のセキュリティ・モデルは、ゼロデイ保護を提供し、コストのかかる侵害や攻撃による悪評の可能性を低減するのに役立ちます。

Rimini Street®

Rimini Protect™でアプリケーション・セキュリティへの「スマートパス」を歩みましょう。

RiminiProtect™は、エンタープライズ・ソフトウェア・アプリケーション、ミドルウェア、データベース、知的財産 (IP) に対して高度なセキュリティ保護を提供する独自のセキュリティソリューションとアドバイザリー・サービスをセットにしたものです。

Rimini Protect™は、お客様が技術ポートフォリオで「スマートパス」を歩むことを支援し、より良い事業成果を実現するための専門知識を提供します。

Rimini Protect™ アドバイザリー・サービスは次の通りです。

- ハードニング・ガイド
- セキュリティ脆弱性分析レポート (SVAR)
- セキュリティ評価

Rimini Protect™ 常時稼働ソリューションと24x365マネージド・サービスを含み、以下のソフトウェアに対しゼロデイや多層防御を実現します。

- OracleやSAPアプリケーション
- Oracleミドルウェア
- Oracle、SAP、オープンソースデータベース (PostgreSQL、MySQL、MariaDB、MongoDB)

詳細はこちら：
https://www.riministreet.com/jp/solutions/support-services/security/

Rimini Street®

riministreet.com/jp
contactjp@riministreet.com
twitter.com/riministreet
linkedin.com/company/rimini-street

リミニストリートについて

リミニストリート（Nasdaq: RMNI）は、エンタープライズソフトウェア製品とサービスのグローバルプロバイダーであり、OracleおよびSAPのソフトウェア製品に対する第三者保守サポートにおいて業界をリードしており、またSalesforce®のパートナー企業でもあります。®リミニストリートは、エンタープライズソフトウェアライセンシーにおいて、大幅にコストを削減し、イノベーションのために資源を自由にし、より良好な業績結果を達成することが可能となる、プレミアムで、非常に応答性が高い、統合型アプリケーションマネジメントおよびサポートサービスを提供しています。業界を問わず、フォーチュン500のグローバル企業、中堅企業、公共セクター組織等を含む顧客が、信頼できるエンタープライズソフトウェア製品とサービスのプロバイダーとしてリミニストリートにサポートを委託しています。