セキュリティ・スポットライト：人的ミスのコストと自動化のメリット

政府機関がセキュリティ管理に対する手作業のアプローチを見直している理由と、インテリジェントな自動化でコストの高いセキュリティギャップから生じる潜在的な脅威を防止する方法

次へ

このeブックの内容

01 はじめに：増大するサイバー犯罪の脅威

サイバー犯罪は増加しています。前年度において、Australian Cyber Security Centre (ACSC) は 67,500 件を超えるサイバー犯罪の報告を受けました。これは前年比で 13% の上昇で、申告された損失は総額で 330 億ドルを超えています。[3] これらのインシデントのうち、およそ 1/4 がオーストラリアの重要なインフラストラクチャに関連する組織に影響を与えました。

政府機関が新しいテクノロジーを取り入れてハイブリッドモデルの働き方に適応していくにしたがって、サイバー攻撃者もその能力を変革させています。従業員やコンピューティング・リソースの分散化が進み、IT インフラストラクチャを取り巻く環境が急速に進化したことで、悪意のある人物がセキュリティのギャップや脆弱性を悪用する新たな機会が生じています。そのため、データ侵害による組織上のコストが上昇しています。このような環境にあっては、強力なセキュリティ体制を構築した組織であっても、リスクの増大は避けられません。

サイバー犯罪に対するプロアクティブなセキュリティ

保護されたシステムやデータを侵害する新たな方法をサイバー犯罪者が考え出しているため、組織はより戦略的でプロアクティブな保護を開発するよう、内外からのプレッシャーを受けています。事実、組織のデータセキュリティやプライバシー対策は、より包括的な規則および法令に順守しなければなりません。

たとえば、豪ニューサウスウェールズ州 (NSW) の Cyber Security Policy では、ACSC Essential Eight リスク緩和戦略に対する成熟度評価の実装と対応が義務付けられました。[1] また、Security Legislation Amendment of Australia's Critical Infrastructure Bill では、重要なインフラストラクチャの管理または運用を担う政府組織に対する規制上の義務が増加する可能性があります。[2]

防御機能の強化

サイバーセキュリティの強化を目指すには、まず既存の脆弱性を特定する必要があります。包括的な戦略がすでに実施されていても、人的ミスとトレーニング不足がセキュリティ侵害を招くことが多々あります。小さなミスを放置しているとシステムへのリスクが生じ、すでに複雑な問題をさらに悪化させます。この結果、信頼性の向上とリスクの低減を目的として、セキュリティ戦略への自動化の導入が進んでいます。

この e ブックでは、人的ミスによって生じたリスクがサイバー犯罪に対する対応にどのように影響するかを確認します。また、サイバーセキュリティの主要なリスク軽減戦略を自動化すると、セキュリティが強化され、IT チームの負担となる時間のかかるタスクの量が低減されることを説明します。

オーストラリアでのサイバー犯罪のコスト

67,500

報告されたサイバー攻撃[3]

330 億ドル

申告された損失額[3]

13%

攻撃数の前年比の増加率[3]

1. Government of New South Wales、「DCS-2021-02 NSW Cyber Security Policy」、2021 年 2 月。
2. Parliament of Australia、「Security Legislation Amendment (Critical Infrastructure) Bill 2021」、2021 年。
3. 「ACSC Annual Cyber Threat Report 2020-21」、Australian Cyber Security Centre、2021 年 9 月。

02 効果的なセキュリティ戦略には全員の関与が必要

人間にミスはつきもの

IT チームのメンバーであっても、システムの脆弱性やそれによるセキュリティリスクを過小評価したり誤解したりすることがあります。リスクを正確に評価できないと、組織にコスト面で大きな損害を与えかねません。

たとえば、ある技術者がファイアウォールを手作業で更新するとします。小さな 1 つのミスをしますが、その技術者は問題になるとは考えず、この脆弱性は対処されないまま残ります。技術者たちには、このような小さなミスによって組織の IT システムに重大な脆弱性が発生するという認識がありませんが、このような隙はサイバー犯罪者にすぐさまつけ込まれてしまいます。

このシナリオでは、技術者の小さなミスから、データの漏洩、業界および政府のデータセキュリティ規制への違反、サービス停止、システムのダウンタイムなど、さまざまな好ましくない結果が引き起こされ、そのコストはすべて組織に降りかかります。

セキュリティにはアプリケーションへのパッチ適用、ファイアウォールの更新、管理者権限の設定と適用など数多くの要素がありますが、これらを手作業で処理するとエラーの入り込む余地が生まれます。また、脆弱性を特定するサイバー犯罪者の能力が高くなっているため、運用チームのみに頼ってこれらのセキュリティタスクを処理していると、好ましくない結果や修復できない結果に至る可能性があります。

人材不足はセキュリティギャップを悪化させる

サイバーセキュリティスキルを持つ人材は需要に追いつかず、手作業による人的ミスの発生確率は高まるばかりです。セキュリティリスクの評価と対処のスキルを持ち、トレーニングを受けた人材が不足しています。(ISC)^2 Cybersecurity Workforce Study によると、オーストラリアではサイバーセキュリティのギャップを解消するには 25,000 人以上の IT セキュリティ担当者が必要です。[4]

このようにサイバーセキュリティ専門家が慢性的に不足しているため、政府機関がリスクを適切に管理することが一層難しくなっています。IT チームはすでに手一杯で、セキュリティプロセスを組織全体に適用する時間がありません。そもそも、プロセスを確立させることすら困難です。

セキュリティチームへの自動化の導入

手動のセキュリティプロセスとスキル不足の双方から高まるリスクへの対処は、サイバー犯罪への対策にとって必須となりました。そして、それに対する有望な解決策が自動化ソリューションです。これから見ていくように、セキュリティプロセスを自動化することで、組織が望んでいた一貫性、精度、スケーラビリティが手に入ります。

手作業でセキュリティ対策を行うことのリスク

「2021 年、セキュリティを自動化していない組織ではデータ侵害によるコストが平均で 671 万ドル発生しましたが、セキュリティ自動化を完全にデプロイした組織では平均して 290 万ドルでした」[5]

4. 「A Resilient Cybersecurity Profession Charts the Path Forward」、(ISC)^2 Cybersecurity Workforce Study、2021 年。
5. 「Cost of a Data Breach Report 2021」、IBM、2021 年。

03 リスク管理の一般的な課題

政府機関にはより優れたリスク管理が必要

公的な情報の機密保持、整合性、可用性を確保するため、政府機関はリスクを正確かつ効率的に特定し、管理できなければなりません。セキュリティ脅威は絶えず進化しているので、組織のリスクプロファイルとセキュリティ体制もそれに常時対応できなければなりません。このような課題に迅速に対応するには、運用の自動化が極めて重要です。

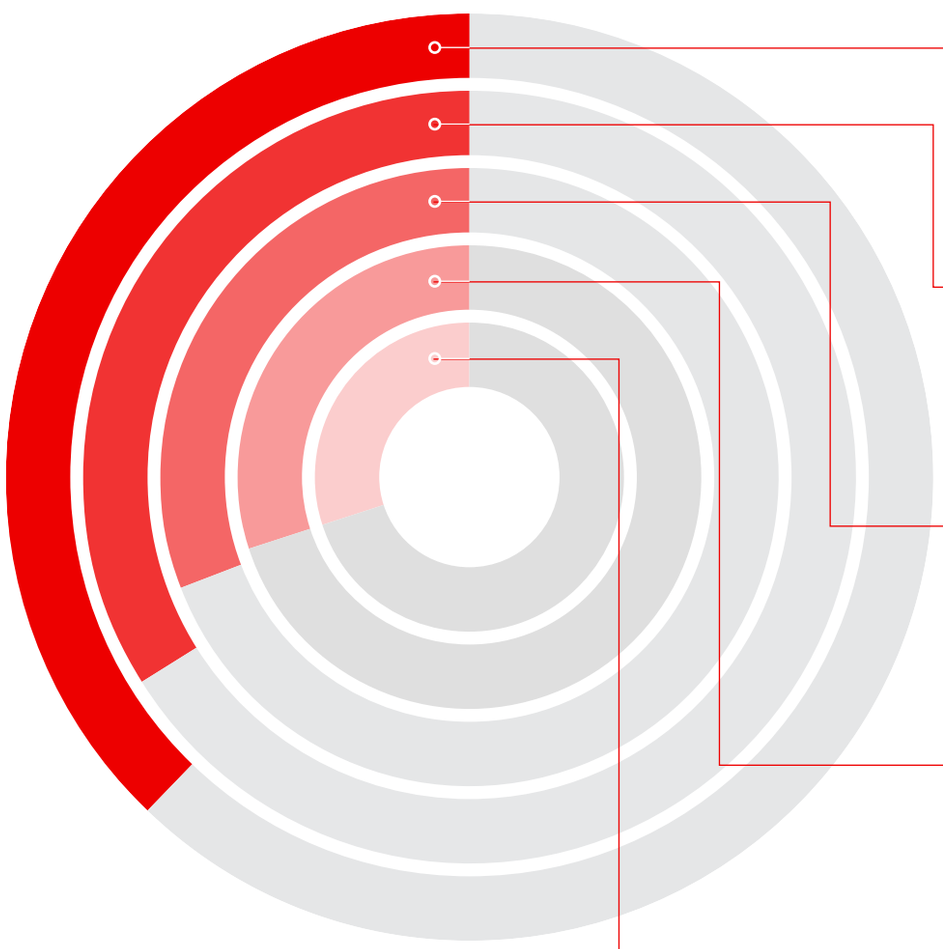
セキュリティ手法の変更を阻む要因

セキュリティを強化しようとする政府機関にはさまざまな課題が立ちはだかり、中でも特徴的な課題は変化の管理に関連するものです。一般的な問題は次のとおりです。

- 新しいサイバーセキュリティの取り組みを実装するには、チームをどのように拡大するのか
- 新しいセキュリティプロトコルに準拠させるには、組織のさまざまな部門をどのようにサポートするのか
- 重要なサービスを提供する既存システムのセキュリティを向上させ、組織が必要とする先進的なセキュリティ戦略を導入するには、何ができるか
- 現在のアーキテクチャでゼロトラストなどの戦略を実装できるか

しかし、これらの検討事項を負担と考えるのではなく、セキュリティの状況の変化を活用してセキュリティ手法を見直し、より厳格なプロトコルを実装するチャンスと捉えることもできます。

サイバーセキュリティの一般的な課題



38%

急速に変化する脅威の状況の把握[6]

34%

リスクや行動に関する教育[6]

31%

内部のサイバーセキュリティ体制の強化[6]

30%

サイバーセキュリティのトレーニングが必要[6]

30%

データ侵害による法的/財政的影響[6]

6. 「State of the Channel 2021」、CompTIA、2021 年 8 月。

04 自動化によるセキュリティ体制の強化

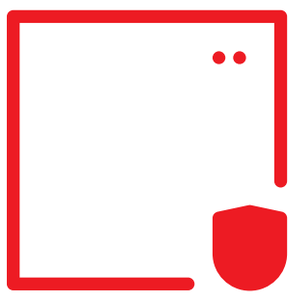
サイバーセキュリティ戦略の主要要素の自動化

リスク低減とサイバー犯罪対策の方法として、政府機関はサイバーセキュリティの自動化に目を向けています。定型的な繰り返し作業を自動化すると、セキュリティチームはより重要で戦略的なタスクに専念できます。さらに自動化は、人的ミスが発生しやすく、セキュリティ上のリスクを増加させるタスクや仕事量を減らし、IT チームが過負荷にならないようにする手助けにもなります。

ACSC Essential Eight は、自動化を使用してサイバーセキュリティ戦略を支援する方法を説明しています。Essential Eight の実装に際して、多くの組織が、人的ミスを一貫して削減または排除する方法がないことで苦労します。現在のリソースに制約があり、技術スキルにギャップがある場合はなおさらです。

IT リーダーは、この問題への対処として、セキュリティ・フレームワークのいくつかの要素を自動化することは可能であり、またそうすべきであると認識しています。以下の例は、組織に自動化を導入する方法や、導入が有意義である場面を示しています。

ACSC Essential Eight の自動化

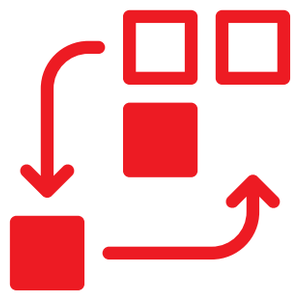


アプリケーション制御

ハイブリッドクラウド上でアプリケーション制御の状態の変更を自動化

アプリケーションおよびオペレーティングシステムのパッチ適用

プレフライトチェック、コンテンツプロモーション、アップデート後の検証およびテストを自動化



バックアップとリストア

バックアップ、リストア、検証テストを自動化

パッチ適用のプロセスの改善

Essential Eight では、攻撃防止に役立てるため、定期的にアプリケーションにパッチを適用し、定期的にアップデートを適用して、セキュリティ問題の悪用から保護することを推奨しています。アップデートが公開されたらすぐにアプリケーションにパッチを適用することはベストプラクティスであるばかりか、多くの場合、規制要件にもなっています。それでも、手作業でパッチを適用すると人的ミスが発生しやすくなり、大規模組織では特に、長時間を要することになります。

パッチ適用は自動化ワークフローのまたとないユースケースです。テストの実行、プレフライトチェックのセットアップ、パッチ適用の実行を IT 担当の従業員に任せる代わりに、検証とテストを自動化できます。このようにすると、これらのすべてのステップが円滑かつ効率的に進行し、その背後では適切なセキュリティが施行されます。

管理用権限の管理

攻撃の範囲を制限するため、Essential Eight では管理用権限の制限を推奨しています。特権アクセスを制御すると、インフラストラクチャおよびアプリケーションにセキュリティがもたらされ、ビジネスプロセスが効率的に実行され、機密データと重要なインフラストラクチャの機密保持が維持されます。

全体的な制御能力は組織内のごくわずかな人々だけが持つべきです。誰に特権を持たせるかの決定は簡単ではありません。セキュリティインシデントの影響範囲を推定し、それによる総合的なインパクトを評価することも同様に困難ですが、この手法を実践すると、誰かが認証情報を悪用した場合に何が起きるかを予測できます。そうすれば、IT チームはセキュリティ対策を実装して、このようなインシデントが組織全体に影響を及ぼさないようにすることができます。

特権アクセス管理ワークフローを自動化し、アクセス認証情報を一元的に保存すると、流出が発生する可能性があるアプリケーションにこれらを挿入する必要がなくなるので、プロセス全体の管理性と信頼性がさらに向上します。

05 サイバーセキュリティのアプローチにおける Red Hat の役割

将来を見据えたサイバーセキュリティ手法の構築

Red Hat® ソリューションは、既存の手作業のプロセスの自動化をサポートできるので、人員不足の IT チームが過負荷で見落しを起こすリスクを低減できます。Red Hat のオープンソース製品はクラウド環境およびアーキテクチャに柔軟性とスケーラビリティをもたらし、現在および将来の環境におけるデプロイメントをサポートします。

サイバーセキュリティ成熟度モデルの基盤に自動化を使用すると、実践的な措置を講じてすばやく反復的に自動化のレイヤーを追加し、手作業のプロセスを置き換えられます。Red Hat ソリューションはリスク軽減と応答の両面で力になります。

Red Hat Ansible Automation Platform

Red Hat Ansible® Automation Platform は Ansible で構築されています。これは人間が読める形式の自動化言語で、複雑な手作業のプロセスを自動化ワークフローに転換します。Ansible Automation Platform により、IT チームは組織内のさまざまなセキュリティプロトコルを自動化し、統合できます。このプラットフォームを使用すれば、精選されたモジュール、ロール、Playbook のコレクションを通じて、調整かつ統一された方法で脅威を調査し、対応できます。

Red Hat Ansible Automation Platform により、次の作業を自動化できます。

- 共通脆弱性識別子 (CVE) のパッチ適用
- アプリケーション制御のロールアウト
- バックアップとリストア、または検証プロセス

Ansible Automation Platform は、ハイブリッドクラウドからエッジ環境まで、大規模な IT 自動化を構築して運用するための、セキュリティ重視で安定したエンタープライズ・フレームワークを提供します。この自動化ソリューションにより、開発者や運用チームからセキュリティおよびネットワークチームまで、組織全体のユーザーが Ansible Playbook を作成、共有、管理できます。IT 管理者は自動化をどのように適用するかのガイドラインを個々のチームに提供でき、自動化の作成担当者は既存の知識を使用するタスクを作成できます。

さらに、Ansible Automation Platform には CyberArk、IBM、Splunk などの認定パートナーからのコンテンツが含まれているので、セキュリティ・ソリューションの統合ポイントとして機能できます。これらのコンテンツはセキュリティ・テクノロジーの管理や統合の自動化に使用できます。

Ansible Automation Platform の詳細はこちら ›

Red Hat Enterprise Linux

Red Hat Enterprise Linux® は、既存のアプリケーションを拡張し、ベアメタル、仮想、クラウド、およびエッジにわたるフットプリントで先進テクノロジーを展開するための基盤を提供します。

Red Hat Enterprise Linux はセキュリティの課題に対処するため、次の 3 点からなる実践的なアプローチを採用しています。

- 軽減：会社のデータやシステム、あるいは評判が危険にさらされる前に、セキュリティを管理し、侵害のリスクを軽減します。
- 保護：最小限のダウンタイムでセキュリティ制御を大規模に自動化し、長期にわたって維持します。
- 準拠：規制の厳しい環境を備えた組織のコンプライアンス基準を最適化します。

Red Hat Enterprise Linux には Information Security Manual (ISM) や Essential Eight などの ACSC ガイダンスに準拠する組み込みのセキュリティポリシーも含まれているため、新しいデジタルサービスへのセキュリティ制御のロールアウトを簡潔かつ一貫して自動化することで、政府機関によるリスク管理の向上を支援します。

Red Hat Enterprise Linux の詳細 ›

Red Hat

前へ

Red Hat でセキュリティを強化

Red Hat はデジタルサービスのセキュリティ向上をお手伝いします

Red Hat は、ACSC のガイダンスを自動化し、自動化されたセキュリティ統合によってリスク管理の向上を支援します。

詳細については、今すぐお問い合わせください ›