ActualTech MEDIA

Hewlett Packard Enterprise

セキュリティ脅威の一歩先を行く

Ed Tittel

目次

はじめに

この技術概要では、HPEおよび認定パートナーの製品やサービスを利用して、中堅・中小企業がセキュリティ問題を未然に防止する方法について説明します。中堅・中小企業にも、リスクとなる脅威や脆弱性を特定し、深刻度に応じて優先順位を決定したうえで、リスク軽減策や対応方針を策定する能力が求められており、変化し続ける脅威に継続的に対処していく必要があります。

本書の主な内容:

- ビジネス目標に対応したセキュリティ戦略の策定
- 「セキュリティファースト」の企業文化の醸成
- 攻撃対象領域の監視とプロアクティブな対応による攻撃の未然防止

「百の治療より一の予防」ということわざは、サイバーセキュリティにもよく当てはまります。治療、つまりセキュリティインシデントやセキュリティ侵害によって生じる問題に対応するためのコストが増大し、今や多くの企業（特に小規模企業）の存続にも関わる脅威となっています。

そのため、セキュリティ脅威や脆弱性がもたらす危険を認識して予測することが極めて重要となっており、次のようなリスク管理の必要性が高まっています。

- 脅威や脆弱性が明らかになったとき、まずは、実際にビジネスのリスクとなるものを**特定**し、そうした脅威がもたらす影響や結果を見極める
- リスクとなる脅威や脆弱性の**優先順位を決定**し、最もコストのかかるもの、または最も深刻な影響をもたらすものから順に対応していく
- 相当のリスクがある脅威や脆弱性に対する**リスク軽減策や対応方針**を策定する

実際には、特に社内にセキュリティ部門を設置することが困難な小規模企業の場合、脅威に関する情報収集と対応をサポートする何らかのサービスを利用することになります。HPEと認定パートナーでも、包括的なセキュリティサービスの一環として、リスクの特定と優先順位の決定、リスク回避などをサポートしています。

すべてを変えるクラウド - セキュリティも例外ではない

さまざまな組織がクラウドのサブスクリプションやサービスを提供する一方で、企業のセキュリティ環境に影響する脅威ベクトルも新たに登場するため、セキュリティ戦略を強化し、組織のセキュリティ対策やサイバーレジリエンスを向上させる措置を講じることが不可欠となっています。企業はこうした目標を達成するために、次のような課題に取り組む必要があります。

- **ビジネスの優先事項に対応したセキュリティ戦略を策定する:** ビジネス上の優先事項とサイバーセキュリティ上の優先事項とのずれを把握することで、経営幹部と関係者双方の戦略を調整し、重要事項に重点を置きながらリソースと予算を配分できるようになります。重要なのは、ビジネスリーダーたちが優先事項について合意し、リスクの全体像を明確に把握していることです。
- **「セキュリティファースト」の文化を醸成する:** セキュリティファーストの文化に価値を置くことが、不確実性やリスクに満ちた世界で成功するための重要な一歩となります。重要資産の保護は、誰もが取り組まなければならない課題となっています。サイバーリスクの発生源と言われるスタッフのセキュリティ意識向上トレーニングに予算を割くことは必要不可欠であり、総力を挙げてサイバー脅威に対処することがビジネスに大きなメリットをもたらします。
- **攻撃対象領域を把握し、ハッカーが見つける前に脆弱性を修正する:** サイバー脆弱性分析（英語）（セキュリティテストやペネトレーションテストとも呼ばれる）は、組織のセキュリティ対策を評価する検証プロセスの1つであり（**図1**参照）、攻撃者が悪用する前に脆弱性を特定します。このプロセスでは、組織内および組織外の視点から、組織の資産が抱えるリスクについて有益な情報が提供されます。また、正式なコンプライアンス評価や監査が行われる前に、セキュリティの不備を特定できます。組織のセキュリティ対策を強化する場合、実行可能なリスク軽減策を立てることも重要ですが、HPEと認定パートナーなどの実績のあるパートナーと連携すれば、自社に不足しているサイバースキルを補完して脆弱性を軽減することができます。

図1: ペネトレーションテスト（侵入テストとも呼ばれる）の4段階

用語の説明

ディザスタリカバリ: 障害が発生した場合、またはアクセスやサービスが全面的に停止した場合でも、企業が通常運用を再開できるサービスやシステムをいいます。

ランサムウェア: あらゆるデータを暗号化して使用不可能にすることで、企業がシステムやデータにアクセスできないようにするマルウェアの一種です。攻撃者側は身代金を支払えばすべてが攻撃前の状態に戻ると主張しますが、FBIは、元に戻る保証はないため、身代金を支払わないよう警告しています。

仮想化/コンテナ化アプリケーションおよびデータ: 仮想マシンまたはコンテナで実行されているアプリケーションやデータ。その多くは、通常は従量制のコンピューティングモデルの一部として、クラウドで運用されています。

エッジからクラウドまで: ビジネスの中心となるオンプレミスのデータセンターやサーバールーム、リモート拠点のネットワークエッジ、または1つ以上のクラウドプラットフォーム（たとえばAmazon Web Services、Microsoft Azure、Google Cloud Platformなど）にあるコンピューティングリソースおよびデータをいいます。

ハイブリッド/マルチクラウドのケース: ハイブリッドクラウドには、コンピューティングのタスクを効率的に処理するために、ローカルとクラウドベースのコンピューティングリソースを単一の環境に統合するケースも含まれます。マルチクラウドは、2つ以上のクラウドプラットフォームが含まれる点を除いて、ハイブリッドクラウドと同じものを指します。今日の多くの企業はハイブリッドマルチクラウド環境でビジネスを行っており、コスト、セキュリティ、パフォーマンスの観点から、最も合理的と思われる場所にワークロードやデータを配置しようとしています。

重要なのは、ビジネスリーダーたちが優先事項について合意し、リスクの全体像を明確に把握していることです。

HPE（および認定パートナー）がIT環境を保護

簡単に検証可能ですが、HPEのサイバーセキュリティソリューションは包括的で革新的かつ堅牢な設計となっています。ハードウェアレベルから始まるセキュリティ機能が、ネットワークエッジにあるユーザーやシステムまで保護します。ソリューション全体としては、セキュリティに関する情報を収集および分析することで脅威に対応するとともに、事業用のシステムやサービスを保護し、セキュリティリスクの管理と最小化についてお客様にアドバイス（および支援）できるように設計されています。

HPEのサイバーセキュリティソリューションは包括的で革新的かつ堅牢な設計となっています。ハードウェアレベルから始まるセキュリティ機能が、ネットワークエッジにあるユーザーやシテムまで保護します。

サーバーから始まるHPEのセキュリティ機能

HPEは、世界標準の安心サーバーを提供するベンダーとして評価されており、HPEのProLiantサーバーファミリは、次のような特徴により、数々の賞や称賛を勝ち取ってきました。

- **保護:** Silicon Root of Trust、Trusted Platform Module（TPM）の機能強化、多層型の改ざん防止、「セキュリティファースト」機能を向上させる「Integrated Lights-Out」（iLO）ファームウェアなどのHPEの新たなイノベーションを通じて、ハードウェアレベルとファームウェアレベルで攻撃を回避します。
- **検知:** ハッキングの恐れのある、または実際にハッキングされたファームウェアコードをiLOが消去し、（可能であれば）既知の有効なコピーに置き換える、ブート整合性チェックなどのあらゆるイノベーションにより、実行時の脅威を検知して回避します。修復できないことがわかった場合は、システムの起動を許可しません（ルートキットなどの目立たないファームウェアベースの攻撃に対する起動前保護を実施します）。

- **復元:** 改ざん防止、暗号化バックアップ、安全かつ確実なリストア手法などの堅牢な機能により、システムを修復して最後の正常な稼働状態に復元させます。

Zerto

HPEは2021年に、ディザスタリカバリ、ランサムウェア攻撃からの復旧、マルチクラウドモビリティソリューションを専門とするZerto社を買収しました。HPEの一部門となったZertoは、エッジからクラウドまでの仮想化/コンテナ化アプリケーションおよびデータを対象とする、継続的なデータ保護およびリカバリ機能を提供しています。お客様はZertoにより、攻撃直前の状態まで瞬時に復旧し、障害発生に伴う時間およびコストの損失やデータ損失を防ぐことができます。Zertoは、従来のデータ保護ソリューションに比べて管理負荷を大幅に低減することで可用性を向上させます。また、Zertoのデータ管理は一元的でスケーラブルかつ自動化されており、クラウド間でワークロードやデータを簡単に移動できます。Zertoは、ハイブリッドクラウド戦略を導入している組織に継続的なデータ保護機能を提供しており、350を超えるマネージドサービスプロバイダーのネットワークによるDisaster Recovery as a Service (DRaaS) も提供しています。テクノロジーを活用してデータ損失やアプリケーションのダウンタイムをゼロに近づける方法については、HPE/ZertoのWebページをご覧ください。

HPEのセキュリティソリューション

HPEのすべてのセキュリティツール、テクノロジー、およびソリューションには、設計、開発、製造、メンテナンスを通じて、3つの主要なアプローチが採用されています。各アプローチの詳細は次のとおりです。

- **データ中心のセキュリティ:** データの保護を最優先するセキュリティ対策です。何らかの機密情報 (個人情報 (PII)、アカウントとパスワード、財務情報や医療情報といった法律上保護されるデータなど) が含まれる場合は特に重要となります。このアプローチは、どのユーザーが何の目的でシステムやデータにアクセスできるのかに重点を置く、次のアプローチに直結しています。

> **HPEと認定パートナーなどの実績のあるパートナーと連携すれば、自社に不足しているサイバースキルを補完して脆弱性を軽減することができます。**

- **ゼロトラストセキュリティ:** 米国国立標準技術研究所 (NIST) はゼロトラスト (英語) (ZT) について、次のような警句を使って説明しています。「Never trust; always verify (何も信頼せず、常に確認せよ)」。ZTはデータとサービスの保護に重点を置いていますが、すべての資産 (デバイス、インフラストラクチャ構成要素、アプリケーションに加え、仮想およびクラウドのリソース) と対象 (ユーザー、アプリケーション、サービス、システム) を含める必要があります。基本的にZTでは、常に攻撃者が存在し、活動していると考えます。このため、誰に対しても暗黙の信頼を示すことなく、常に資産や業務へのリスクを分析して評価します。ユーザーに必要最低限の権限のみを付与する「最小権限の原則」(PLP) を適用するなど、すべてのアクセス要求に対して本人確認を行うことが主な戦略となります。

- **DevSecOps:** 開発者 (および試験者、文書作成者、トレーナーなどのサポート担当者) と運用スタッフ (管理者、テクニカルサポート、フィールド技術者、修理担当者) を単一の組織にまとめて目標や目的を共有させる、DevOpsのアイデアを拡張したものです。DevSecOPsはDevOpsをさらに発展させ、1つのセキュリティチームが開発ライフサイクル全体をサポートすることで、企業のIT運用の各段階 (設計、構築、テスト、メンテナンス、および廃棄) でセキュリティが考慮されるようにします。

ソリューションの枠を超えた、エキスパートによるコンサルティングサービス

HPE Pointnext Servicesでは、中堅・中小企業におけるセキュリティ戦略の監査、定義、改善をサポートしています。Pointnextのエキスパートが、セキュリティポリシーの策定だけでなく、プライバシー、機密保持、データ保護に関するコンプライアンス要件への対応も支援します。また、リソースや専門知識が不足している企業でも、低コストで効果のあるソリューションを統合し、事業継続性やディザスタリカバリを実現できるようにサポートすることが可能です。実際にPointnextは、企業がセキュリティ設計の基盤となるセキュリティ戦略を策定し、予算の範囲内で確実

に実装できるようにサポートすることを得意としています。また、テスト、パイロット、本番環境を通じて、エンドツーエンドに支援することが可能です。このようにPointnextなら、リモートワーカー、エッジ、オンプレミス、ハイブリッド/マルチクラウド環境を含む組織全体にセキュリティが確実に組み込まれるように企業をサポートすることができます。

サプライチェーンの保護

HPEが運用するTrusted Supply Chain (TSC) は、通常よりも厳格なセキュリティ要件やユースケースに対応しなければならないお客様向けのサービスです。このサプライチェーンの代表的なお客様として、検証可能な製品保証の付いた米国製の製品の調達を義務付けられている米国連邦政府や公的機関が挙げられます。TSCには2つの主要な方法でセキュリティが直接組み込まれています。まず、対象となる製品には、改ざん防止のための高度なセキュリティ機能が搭載されています。次に、HPEがサプライチェーン全体を監視し、すべての部品を承認して組み立てを確認することで、お客様に納品されるまで包装された製品のセキュリティを維持し、改ざんを防止します。

Project Auroraは、シリコンレベルから始まる新しい組み込みの統合セキュリティソリューションを提供する、包括的なセキュリティアーキテクチャーです。Project Auroraがサプライチェーンで活用され、署名や大きなパフォーマンス上のトレードオフ、ロックインを必要とすることなく、インフラストラクチャからオペレーティングシステム (OS)、ソフトウェアプラットフォーム、ワークロードに至るまでの変更不可能な信頼のチェーンを確立する仕組みをご確認ください。

HPEのすべてのセキュリティツール、テクノロジー、およびソリューションには、設計、開発、製造、メンテナンスを通じて、3つの主要なアプローチが採用されています。

HPEと認定パートナーでは、中堅・中小企業のお客様がリスクを管理し、システムとデータを保護するとともに、今日の複雑で困難なセキュリティ環境に対処するうえで役立つ、各種の高度なセキュリティソリューションを提供しています。詳細については、HPEの中堅・中小企業向けITソリューションのページをご覧ください。また、小規模企業の安全とセキュリティの維持をサポートするために、サービス部門であるPointnextを通じてHPEおよび認定パートナーが提供する、コーチング、コンサルティング、サポートなどの各種サービスの利用もご検討ください。