AWS セキュリティ

セキュリティのカルチャーを構築する

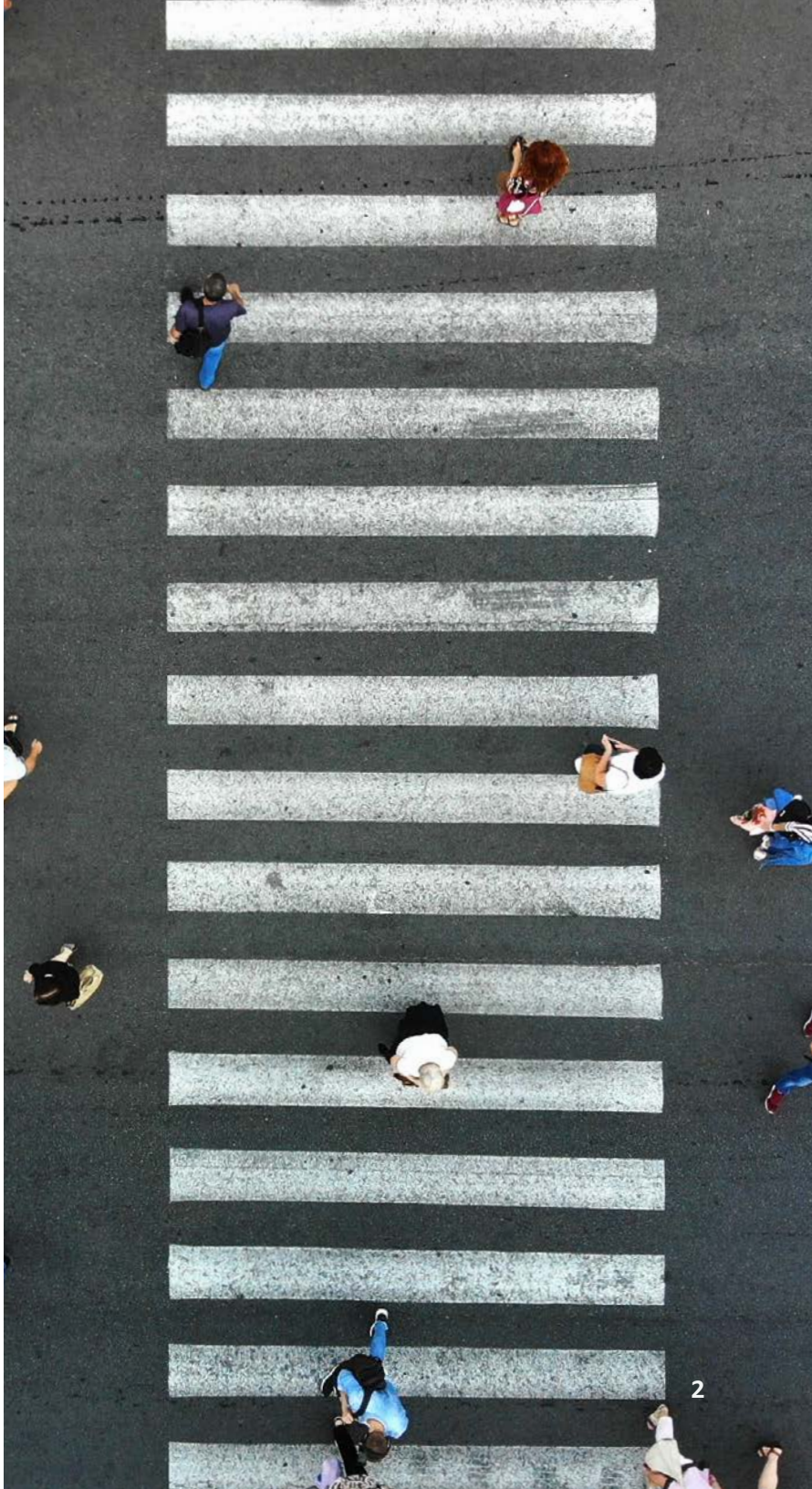
アマゾン ウェブ サービス (AWS)
エンタープライズストラテジスト
兼エバンジェリスト
Mark Schwartz

強固になるとは、予期しない事態が発生した際の回復力を持つこと

企業のリスク体制を監視し、一連の制限ポリシーを通じてそれを管理するスペシャリストのチームにセキュリティを任せておくだけでは、もはや十分ではありません。企業のネットワーク境界をファイアウォールで保護したり、コンプライアンスフレームワークで指定された一連の統制を実装したりするだけでは不十分です。セキュリティは全員の仕事となり、その管理は企業にとって戦略上の懸念事項となっています。セキュリティカルチャー、リスクと統制の認識、企業を安全に保つための一連の規範や手法を構築していく事が、企業が前進する方法です。

この時点で、セキュリティ関連の読みものではこの後に、不正行為者が悪用できる脆弱性を放置したために、大きな被害に遭った企業の恐ろしい事例を述べるのが通例となっていますが、やめておきましょう。私たちは皆、既にこうした脅威を十分に認識しているからです。それより重要なことは、私たちがビルダーや企業のエグゼティブとして、当たり前に行っている構築、行動、意思決定の手段として、セキュリティを前向きに考えていくことに慣れる必要があるということです。特定の脅威が発生したら受動的に対応するのではなく、カルチャーの一部としてセキュリティを取り扱っていく必要があります。

企業が IT 機能をデプロイするとすぐに、それをハッキングするために数えきれないほどの攻撃が実行されます。しかし、システムに対する脅威の発生元は不正行為者だけではありません。IT システムにとって、質の悪いデータ、使用量の予期しない急増、同時実行オペレーションに関連する未テストのエッジケース、カスケード障害、幾何学数的に加速する速度の問題なども脅威となる可能性があります。システムがジョブを安全に実行するには、スケーラブルで、回復力があり、可用性が高く、十分にテストされていて、パフォーマンスに優れ、耐障害性および予期外の入力に対する耐性を備えている必要があります。



セキュリティは品質の問題

ここで良い知らせがあります。セキュリティは、品質と同じ意味合いで、無料であるとよく言われます。例えば、手洗いなどの基本的な衛生習慣と同様、(ほぼ) 無料です。セキュリティを組み込むことは、後で追加するよりも安く済むという点においてもです。セキュリティは品質の一種なのです。

それは、攻撃を受けたり予想外の事態に直面するような、実際の状態に置かれたとき、IT 機能が設計どおりに継続して機能するよう保証することです。

品質とスピードの間にトレードオフがないように、セキュリティとスピード間にもトレードオフはありません。興味深いことに、これまでのほとんどの攻撃は、簡単なセキュリティハイジーン (衛生管理) で阻止することができたのです。侵入行為のほとんどは、わずかな弱点が原因となって発生します (例えば、技術面に精通したお客様であればおわかりかと思いますが、SQL インジェクションやバッファオーバーフローなど)。

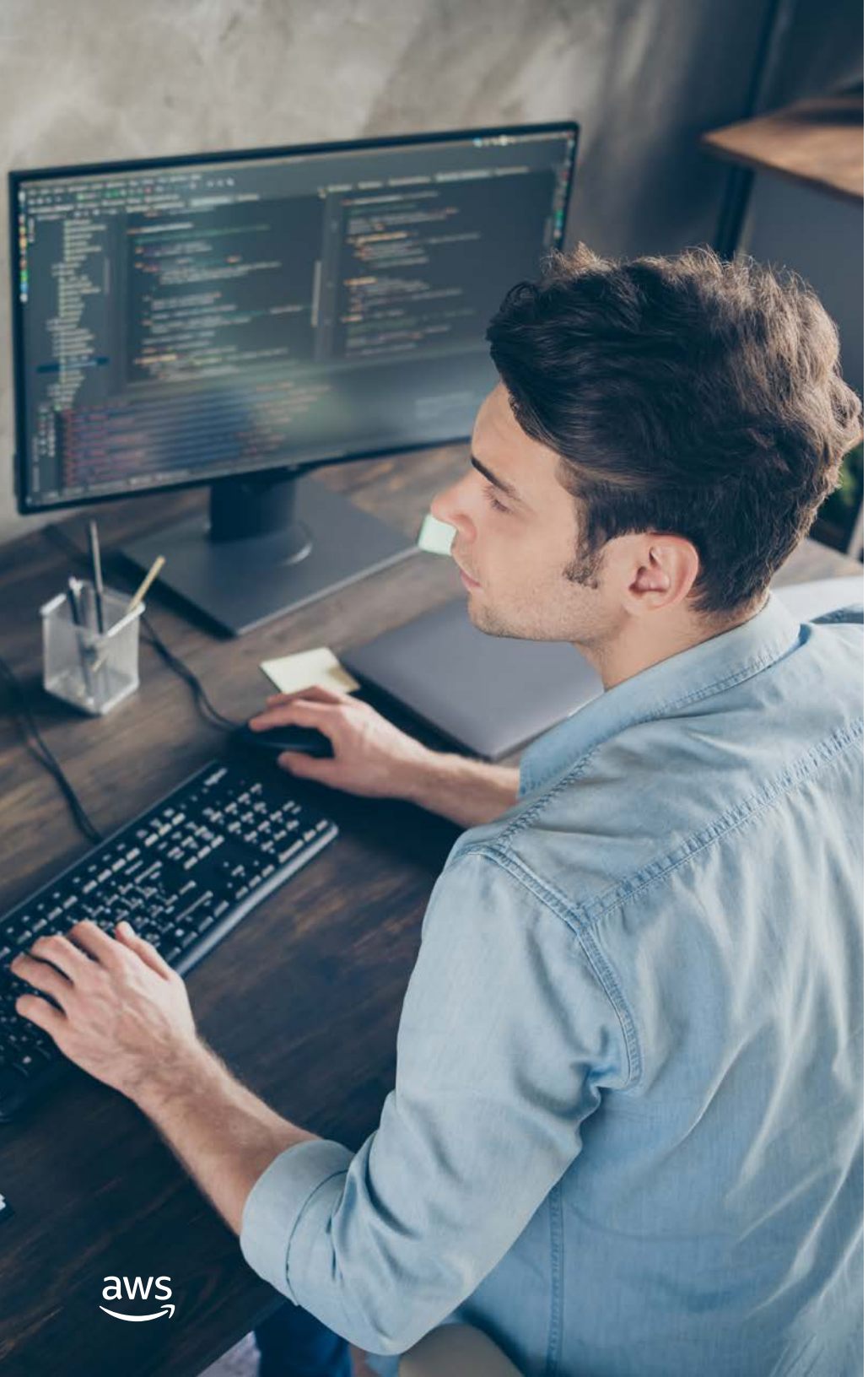
> ***安全なコードを作成するための鍵は、ソフトウェア開発のカルチャーを変革することだと考えています。私たちは、技術に注目するだけでなく、その技術を構築したソフトウェア開発組織にも注目する必要があります。この進化は、その組織の人、プロセス、テクノロジー、カルチャーから始まらなければならないと考えています[1]"***
>
> ***アマゾン ウェブ サービス、エンタープライズストラテジスト兼エバンジェリスト、Mark Schwartz***

セキュリティ上の最大の懸念について CISO に質問すれば、おそらく、認証情報の侵害と、十分頻繁にパッチを適用できないこと、という回答が返ってくるでしょう。これに加えて、主要なアプリケーションの脆弱性 (SQL インジェクションやクロスサイトスクリプティング) があり、それらが実際の侵入におけるほとんどの原因になっています。しかし、最新の優れたプラクティスにより、デリバリープロセスを遅くしたり、ユーザーに過度の負担をかけたりすることなく、これらの脆弱性を回避する安価な方法を得られます。セキュリティは手が込んだマニアックな技術ではありません。日常業務の中で優れたプラクティスに従うことが重要なのです。それは衛生習慣のようなものです。

セキュリティカルチャーとは?

セキュリティハイジーンに基づくカルチャー主導のセキュリティへのアプローチとして私が見つけた最善のモデルは、強固なソフトウェアまたは強固な DevOps ムーブメントのモデルです。これには、適切な対応として、安全で回復力の高いソフトウェアの構築が推奨されています。強固なモデルを作るムーブメントを開始した人たちによれば、「強固な組織は、今日の脅威だけでなく、将来の課題にも同様に対抗できるよう設計された強固なコードを作成している」とのことです。つまり、強固さの鍵はカルチャーだということです。

[1]「The Rugged Handbook」(堅牢化のためのハンドブック)、Strawman Edition、2012 年 8 月



これらの人たちは、コードとソフトウェア開発についても述べていますが、このような原則は企業全体に当てはまります。セキュリティとレジリエンスを「あったらいい」品質として扱う (セキュリティのスペシャリストのみが心配すればよいと考える) 企業、余計なコストや負担として扱う企業、まったく考慮しない企業は、決して強固になることはできません。セキュリティとレジリエンスは、すべての企業のエグゼティブ、マネージャー、従業員にとって懸念事項とされるべきであり、事実そうです。これは、企業文化において基本的なものとされるべきです。カルチャーには、全員の行動、および他人の行動に対する見方によって補強される企業規範が含まれます。

> ***「強固」とは、可用性と存続可能性を備え、防御力が高く、安全で回復力のあるソフトウェアを制作する能力を迅速に進化させるカルチャーを持つ、ソフトウェア開発組織を示します。強固な組織は、同じ過ちを何度も繰り返すのではなく、競争、協力、実験を学習と改善に役立てます。また、脅威を積極的に見つけ出し、問題になる前に防御態勢を築きます。***
>
> ***アマゾン ウェブ サービス、***
> ***エンタープライズストラテジスト兼エバンジェリスト、Mark Schwartz***

強固な組織を目指すうえでの原則

それでは、セキュリティカルチャーとはどのようなものでしょうか。強固な組織に当てはまると思われる、いくつかの原則をまとめました (「*The Rugged Handbook*」(堅牢化のためのハンドブック) から多く引用しています)。

継続する攻撃 : 意図的な攻撃や偶発的な攻撃を継続的に受けていることを理解し、すべての行動にこの考えを組み込みます。

トレーニング : セキュリティに関するトレーニング (職務に応じて、技術的または技術以外のトレーニング) を重視します。増加中の脅威を常に把握し、セキュリティスペシャリストからのアドバイスを受け入れ、セキュリティポリシーとルールの理解に努めます。

セキュリティハイジーン : 優れたセキュリティハイジーンは、適切な業務遂行の一端です。パスワードは公開しません。ユーザーアカウントは共有しません。夜帰宅する際に、デスク上に機密性の高い個人情報を放置しません。安全なコーディング手法を使用します。

継続的な改善 : 夜帰宅するときにデスク上に機密情報を放置しておいた場合、それに気付いた人からの忠告を受け入れ、二度と行わないようにします。

欠陥ゼロのアプローチ : 既知の脆弱性は一切受け入れません。問題を発見した場合は、直ちに修正します。セキュリティ欠陥に優先順位を付けません。つまり、一部は今すぐ修正する必要があり、一部はそうでないというような判断は下しません。

再利用可能なツール : IT システム全体を見渡し、それらのシステム間で共有できるツールとプロセスを構築します。これには、再利用可能なログ記録とモニタリング、企業全体のユーザーのプロビジョニング、従業員向けの標準化されたオンボーディングとオフボーディングプロセスなどが含まれます。

統一されたチーム : 組織のすべての部門は、共同でセキュリティを強力なものにし、回復力のあるシステムを実現します。

テスト : 開発中、および本番稼働中にもシステムを綿密にテストします (主に自動化されたテストを実施)。障害シナリオとそれに対する対応力をテストします。

脅威モデリング : お客様の心境になって考えてみるのと同様に、攻撃者の立場になって考えてみます。自分たちの管理策を打ち破るために攻撃者が取る可能性のあるルートをブレーンストーミングし、それが可能でないことをテストして確認します。

同僚による確認 : 各技術者は、作業に欠陥がある可能性や、セキュリティの脆弱性がある可能性の両方について考える必要があります。コードは、必ず同僚が確認し、同僚もまた、脆弱性を探す責任を持ちます。

> ***“データが利用可能になるまでの速度により、意思決定が下されるまでの速度が決まります”***
>
> ***アマゾン ウェブ サービス、エンタープライズストラテジスト兼エバンジェリスト、Mark Schwartz***

> *セキュリティをミッション (または事業) 達成に不可欠な要素として扱えば、考えられているような多くのトレードオフが発生することはめったにありません”*
>
> *アマゾン ウェブ サービス、エンタープライズストラテジスト兼エバンジェリスト、Mark Schwartz*

USCIS でセキュリティカルチャーを構築した方法

私が米国国土安全保障省の機関である米国市民権・移民局 (USCIS) で CIO を勤めていたとき、私たちはセキュリティについて熟考を重ねました。しかし、私が最初に入庁したときは、セキュリティが全員の日常業務の一部にはなっていませんでした。もちろん、すべての職員がセキュリティ意識向上のため毎年トレーニングコースに合格することが義務付けられていました。きわめて有能なセキュリティエンジニアと侵入テスターがいて、システムを安全に保つために力を尽くしていました。また、定期的にソーシャルエンジニアリング監査を実行しました。

しかし、ほとんどの職員はセキュリティを負担と見なしていたのです。デベロッパーは、コードを本番環境にデプロイするうえで、セキュリティは遅延要素であると見なしていました。「安全」とは、セキュリティテスターの要件を満たし、コンプライアンス要件に合格することを意味していたのです。システムは既知の脆弱性を含んだ状態でリリースされ、それらの脆弱性は後で対応するため、追跡システムにリストされていました。こうした脆弱性の存在を許可することは、「リスク分析」に基づく「ビジネス上の決定」と呼ばれていました。

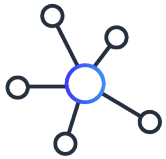
視点を変える

私は CIO として、リリースに際して各システムが十分に安全であるかどうかを決定する承認責任者を務めました。これを行うために、CISO やセキュリティチームと相談し、運用機関としての認定 (ATO) を付与しました。政府の ATO プロセスは、機関に柔軟性を与えるよう意図的に設計されていました。企業の事業執行責任者として、リスクベースのトレードオフを行い、セキュリティが実践的で、ミッション達成と均衡のとれたセキュリティ目標として扱われるようにしました。

残念ながら、このアプローチでは、セキュリティはミッション達成と相反するものであり、トレードオフが必要であるという誤った考えを伝えてしまいます。しかし、セキュリティをミッション (または事業目標) 達成に不可欠な要素として扱えば、考えられているように多くのトレードオフが発生することはめったにありません。

これら 5 つのメカニズムにおいては、多額のコストは発生せず、確立後は、多くの時間を必要としない点を念頭に置いておくことが重要です。これは、セキュリティと成果実現の間のトレードオフではありません。これら 5 つの各メカニズムについて、以下で詳しくご説明します。

USCIS ではセキュリティカルチャーを構築するために、以下のようなアプローチを採用しました。

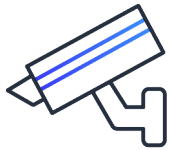


ミッションの目標に一貫してセキュリティを組み込む

すべてにセキュリティを組み込み、間違いは直ちに修正する

セキュリティハイジーンの規範と高い水準を確立する

欠陥ゼロのアプローチを採用する



開発と本番稼働におけるセキュリティを継続的に確認する

ミッションの目標に一貫してセキュリティを組み込む

私たちは皆、システムのセキュリティ維持に関して、お客様や他のステークホルダーに対する責任を負っています。お客様からの信頼を得て、個人情報をお預かりしています。株主からの信頼を得て、企業の財務データをお預かりしています。USCIS の場合、国の移民システムの整合性の維持において、国民からの信頼を得ていました。これらの責任は、リーダーから各メンバーに至るまで、組織内の全員が負っています。

CFO は、セキュリティが財務の健全性にとって重要なことを明確に理解する必要があります。CMO および営業責任者は、企業がそのシステムの整合性を保護することでのみ、顧客に対して暗示的または明示的な約束を守ることができると明確に理解する必要があります。COO は、整合性と一貫性を備えた信頼のある方法で会社を運営しなければならないことを理解する必要があります。

組織内の全員が、セキュリティを重要なジョブ要件と見なす必要があります。全社員が、次のような質問を自問自答する必要があります。「システムが侵害されてもよいのか?」「申請者のデータが盗まれてもよいのか?」「サービス拒否攻撃でサービス提供が停止してもよいのか?」セキュリティが重要であると考えていないのであれば、それは仕事に関する認識が間違っています。

私は、ATO を付与するかどうか決定するため、セキュリティ関係者のみでなく、ビジネススポンサー、プロダクトオーナー、開発チームを含む、すべての主要なステークホルダーとの面会を要求しました。システムのセキュリティ体制を判断するための質問を行い、明らかになった問題について全員が確認し、理解できるようにしました。セキュリティ強化のために実行すると掲げたアクションに対し責任を持つよう人々に要求しました。さらに、調査結果についてセキュリティチームをサポートし、セキュリティに交渉の余地はないことを全員に対して明確にしました。

すべてにセキュリティを組み込み、間違いは直ちに修正する

私たちの定期的な監査により、喜ばしくないニュースが明らかになりました。それは、職員がソーシャルエンジニアリング攻撃に騙されていたということです。どれだけトレーニングしても、職員は「ヘルプデスクの技術者」を名乗る人物からの依頼に対してパスワードを教えてしまいます。熟練した攻撃者であれば、ユーザーを騙してリンクをクリックさせるようなスピアフィッシング攻撃を設計できるでしょう。パスワードに十分な強度を持たせ、システムごとに異なるものにする場合、覚えておくことが困難になるため、ユーザーはパスワードを書き留めてしまいます。

それが、私たちが多要素認証に完全に移行した理由です。多要素認証は万能ではありませんが、プロセスがはるかに簡単になります。私たちは開発パイプラインに自動化されたセキュリティテストを導入し、一般的なセキュリティの脆弱性が発見された場合、脆弱性の内容と回避方法を示したフィードバックが迅速にデベロッパーのもとに送られます。優れたセキュリティ手法 (ID と認証情報管理、監査、ログ記録など) を実装し、新しいシステムに簡単に組み込むことができる再利用可能なコードを作成して、全員のノートパソコンに暗号化ソフトウェアをインストールしました。

侵入テスターが脆弱性を発見すると、全員を集め、テスターに調査結果を提示させ、テスターがどのように私たちを騙したのか、そして同様のインシデントを今後どのように回避できるのかを全員が理解できるようにしました。

セキュリティハイジーンの規範と高い水準を確立する

洗面所から出たら手を洗います。デベロッパーであれば入力を検証します。手を洗うことで、雑菌を体内に取り込む可能性が低下します。入力を検証することで、SQL インジェクションやバッファーオーバーフローなどの攻撃により被害を受ける可能性が低下します。これは常識であり、行わない場合、社会からつまはじきにされてしまいます。

手を洗っても遺伝性神経疾患を防ぐことはできませんが、最も一般的な病気は遺伝性ではありません。同様に、通常のセキュリティハイジーンでは防ぐことができない複雑な攻撃もありますが、これまで攻撃の大半は、私たちが忘れていた簡単なことや、ケアレスミスが被害の原因になっています。

セキュリティハイジーンは、事実上コストがかからず、きわめて効果的です。ほとんどは新しい習慣の構築が問題となりますが、日々のセキュリティ攻撃の大部分を防ぐことができます。重要な書類は、シュレッダーで破棄します。ユーザーアカウントには、可能な限り最小限の権限を付与します。従業員が退職した場合、アカウントを直ちに削除します。

> ***セキュリティハイジーンは、事実上コストがかからず、きわめて効果的です。ほとんどは新しい習慣の構築が問題です”***
>
> ***アマゾン ウェブ サービス、***
> ***エンタープライズストラテジスト兼エバンジェリスト、***
> ***Mark Schwartz***

欠陥ゼロのアプローチを採用する

私には、既知のセキュリティ脆弱性を本番環境で許可するという考えが理解できません。ほとんどのドアに施錠するが、1 つだけ無施錠にするのは何のためになるのでしょうか。泥棒が家に侵入するには、ドアが 1 つあれば事足ります。これはリスクやコストのトレードオフではありません。1 つのドアを無施錠にすれば、その他のセキュリティ関連支出を無駄にすることになります。

継続的デリバリー環境において、コードはプロモーション前にすべてのテストに合格する必要があります。これは合格か不合格かというシンプルな条件です。すべてのセキュリティがこのように扱われるべきです。これは非常に大きな負担であると思われるかもしれません。しかし、多くの未解決のセキュリティ欠陥があるレガシーシステムの場合を除き、自動回帰テストスイートによる優れた手法を導入すれば、どの時点においても、欠陥が存在する可能性のある唯一の場所は、チェックインされた少量のコードのみになります。

USCIS で、私が各レガシーシステムを (部屋にすべての主要なステークホルダーがいる中で) 確認していた際に、存在する既知の脆弱性について尋ねてみました。それぞれの脆弱性の修正計画や、計画実行に向けた補完制御と非常に積極的なタイムラインの確立を主張しました。そしてすべてのステークホルダーが、既知の脆弱性は許容できないという理解に達したのです。

開発と本番稼働におけるセキュリティを継続的に確認する

USCIS のプロセスでは、各システムを 2 ～ 3 年毎に見直し、引き続き安全なことを確認してから、新しい ATO を付与していました。それに代わり、各システムの進行中の認証プロセスへのエンロールを開始し、システムが稼働している間、自動化されたツールにより、そこでシステムの継続的なテストと評価が行われました。

脆弱性が見つかった場合、それに対応する迅速なエスカレーションプロセスがありました。基本的に、リリース前のセキュリティテストプロセスはリリース後に拡張しました。システム起動当初に ATO の付与を阻止していたのと同じものが、今や起動後においても迅速なエスカレーションと修正をトリガーしています。

これにより、セキュリティは必要に迫られて考えるものではなく、事前に考慮するものとなりました。私たちは安全なシステムをリリースするだけでなく、あらゆる時点で、できる限り安全であることを証明したかったのです。別の見方をすると、システムが攻撃を受けたときだけでなく、攻撃を受けやすくなる欠陥が検知されたときにも、緊急性を要するということです。

新しい習慣を構築し、独自のカルチャーを築く

ここに示したテクニックはすべて、セキュリティは重要であり、私たちがステークホルダーに対して責任を負っているものであるというカルチャーの構築に寄与していました。このテクニックでは、古い習慣を破壊し、新しい習慣を作る必要がありますが、コストや時間がかかるものではありません。そして最も重要なことは、それらが安全性と顧客満足の間にはトレードオフが存在するという、問題のある考えを排除するうえで役に立ったことです。

関連コンテンツ

セキュリティに関するリーダーシップの育成

企業の CISO が、どのように従業員への投資を行い、組織を保護しているのかをご確認ください。

AWS セキュリティとコンプライアンスのクイック リファレンスガイド

堅牢なセキュリティと規制コンプライアンスを維持しながら、コスト削減とスケーラビリティを実現する方法をご紹介します。

AWS re:Invent 2019 AWS Security Leadership Session (AWS re:Invent 2019 AWS セキュリティ リーダーシップセッション)

AWS 最高情報セキュリティ責任者の Stephen Schmidt が、クラウドセキュリティの現状についての見解を共有しています。

革新的なリーダーが、ビジネスの成長と変革をどのように推進しているのかをご紹介します。

詳細はこちら ›

著者について

アマゾン ウェブ サービス、エンタープライズストラテジスト兼エバンジェリスト、Mark Schwartz

Mark は、「War and Peace and IT: Business Leadership, Technology, and Success in the Digital Age」(戦争と平和と IT: デジタル時代におけるビジネスリーダーシップとテクノロジーと成功)、「The Art of Business Value」(ビジネス価値を生み出す技術)、「A Seat at the Table: IT Leadership in the Age of Agility」(俊敏性の時代における IT リーダーシップとその立ち位置)の著者でもあります。

AWS 入社前は、米国市民権・移民局 (米国国土安全保障省の機関) で CIO、Intrax で CIO、Auctiva で CEO を務めていました。ペンシルベニア大学ウォートン校で MBA を取得しており、エール大学ではコンピュータサイエンスの学士と哲学の修士号を受けています。Mark は、熱心なブロガーでもあります。

Mark の詳細はこちら ›