セキュリティ監査の読み取り方や説明責任の構築

2020 年 9 月
名和 利男

はじめに

近年、「サイバー脅威の増大」や「攻撃手口の高度化、巧妙化」などのような表現で、組織におけるサイバーリスクが急激に高まっていることが懸念されている中で、残念ながら、国内で事業リスクに直結したサイバー被害が複数発生している。もはや、サイバー攻撃は生産性、評判、知的財産を含む企業資産に大きな影響を与える可能性の高いリスクとなってしまった。そのため、さまざまな業界の企業がサイバーセキュリティの改善および強化の取り組みを始めている。

その取り組みの最初のプロセスにおいて、セキュリティ・インシデントの発生回避、被害抑制、迅速対処、早期復旧を実現するための体制や能力を有しているかどうかを見極めるために「セキュリティ監査」を実施する。具体的には、企業における情報システムについて、セキュリティ対策が特定の水準にどれだけ適合しているかを測定するなどして、情報システムのセキュリティ環境を体系的に評価する。

この評価結果に基づいて、実効性および適正性のあるセキュリティ対策を選択及び集中させることで、サイバー攻撃の脅威に適合した取り組みにつなげていくことができる。

脅威に適合しようとするセキュリティ監査の変化

セキュリティ監査には、実施内容の性質の違いによりいくつかの種類がある。主なものとして、組織のリスクの特定、推定、優先順位付けに役立つ「リスクアセスメント」、セキュリティ手順、設計、実装、内部統制の欠陥を明らかにする「脆弱性評価」、最近のハッキング手法を使用して IT インフラのセキュリティ上の弱点を明らかにする「ペネトレーション（侵入）テスト」、組織が業界でビジネスを行うために必要な規定への準拠状況を確認する「コンプライアンス監査」などを挙げることができる。

これらのセキュリティ監査の手法やプロセスは十分に成熟しており、知識体系や標準的なフレームワークが整備されている。多くの企業は、このようなセキュリティ監査を実施することにより、対外的な説明責任や信頼性の確保に役立ててきた。

しかしながら、サイバー攻撃による脅威が急激に増大したことで、これまでのアプローチによるセキュリティ監査では、組織の事業や資産に悪影響を及ぼす箇所を見過ごしてしまうケースが目立ってきた。この主な要因としては、すでに確立されたセキュリティ監査の設計思想が「単体システム及びその連続したつながり（プロセス）」をベースにしていたことにある。

最近のサイバー攻撃が仕掛けられる対象領域は、「相互に複雑につながったシステム群を基盤とした、エントリーポイント（入り口点）が多数存在するソフトウェアの組み合わせの全て」である。これは、Attack Surface（攻撃表面、攻撃対象領域）という概念で知られているものであるが、これに加えて、ソフトウェアへの依存性を高めている人間の脆弱性（心理のスキ）を悪用した詐欺的行為も増加しているため、このようなリスクへの対策設計は多種多様な要素の組み合わせとなる。そのため、既存のセキュリティ監査を実施しただけでは、これらを体系的かつ網羅的に評価することが困難になってきているのである。

そこで、最近のセキュリティ監査では、「脅威主体が取りうる攻撃のプロセスや手順を踏襲したアプ

ローチ」を取ることで、網羅性や有効性を少しでも高めようとする努力が行われている。実際には、次の 3 つのアプローチがある。

- ブラックボックス監査：監査対象の IT 環境について公開されている情報だけで行うもので、攻撃者がシステムを標的にして侵害しようとする実際のシナリオをシミュレートすることを目的とする。攻撃標的における内部の運用や IT インフラに関する知識を有していない意欲的な攻撃者を完全にシミュレートすることで、標的型攻撃を受けた場合の既存のセキュリティ対策の堅牢性を確認することができる。
- ホワイトボックス監査：実際の従業員の情報など、監査対象に関する可能な限りの内部情報の提供を受けた上で行う。攻撃者がインサイダーや内部からの流出情報によって、内部インフラに関する詳細情報を入手した場合を想定し、最悪のシナリオに備えることを目的とする。また、監査の過程の中で、新たな脆弱性の発見や、重要情報へのアクセス可能性が判明することがある。そのため、ソースコード監査やアプリケーション設計レビューなどにも活用されている。
- グレーボックス監査：意欲的な攻撃者が収集する可能性のある、監査対象に関する内部情報の一部の提供を受けた上で行う。提供される情報には、ポリシー文書、ネットワーク構成図、その他の機微な情報が含まれる。組織にとって重要な領域に焦点を当てながら、費用対効果の高い監査が期待できる。インフラに関する部分的な情報を入手した攻撃者からの脅威を正確にシミュレートすることができ、ソーシャルエンジニアリングやその他のオフライン詐欺によって内部情報が漏洩した場合のシナリオを作ることができる。

このようなアプローチに基づいたセキュリティ監査で得られる最悪のシナリオ（Worst-case scenario）を理解することで、企業が現在利用できるリソースと機会を最大限に活用することができ、不測の事態に備えたビジネスの準備に役立てることができる。

ところが、このようなセキュリティ監査は、高い専門性や豊富な経験を持つ者により実施されるが、その実施者の知識・能力やバイアス*1、および用語の不正確な表現や解釈の違いなどが発生しやすい。そのため、この結果を受ける企業は、サイバーセキュリティ特有の読み取り方や説明責任の構築において留意すべき事項がある。

*1 思考や判断に特定の偏りをもたらす思い込み要因や、得られる情報が偏っていることによる認識の歪み

監査結果の読み取り方と説明責任の構築

セキュリティ監査の結果は、以前までは「種類（分類数）の少ない単純でやや固定化された攻撃手法」を前提としたものがほとんどであったため、セキュリティに詳しくない担当者でも容易に理解することができた。しかし、最近は「種類（分類数）の多い複雑多岐で常に変動する攻撃手法」を前提としたものとなっているため、必然的に実施者の知識や経験に依存した結果になりやすいことに加え、報告として記述された事項に幾つものパターンが発生する。

例えば、二段階認証を実装しているアカウント管理をしている対象へのセキュリティ監査において、同じ対象であるにも関わらず、実施者によって次のような異なる結果が出ることがある。

- 二段階認証により、アカウント管理は十分に行われている。
- 二段階認証により、高いレベルのアカウント管理は行われている。しかし、ワンタイムパスコードを受信するメールアドレスが指定されていない（フリーアドレスの利用を許している）ため、そのメールがアカウントハイジャックや中間者攻撃などを受けている場合、二段階認証が回避される

可能性がある。

- 二段階認証により、平均的なアカウント管理が行われている。しかし、パスワード再発行手続きにおいて、本人確認のための「秘密の質問」の設定に不備がみられるため、第三者に乗っ取られる可能性がある。

これらの違いが発生する主な理由は、実施者が直近のサイバー攻撃の状況を把握し、その発生可能性を理解しているかどうかによるところが大きい。これに加え、利用者目線で、利便性の確保のために実装している機能やプロセス(この例示ではパスワード再発行手続き)に着目した観察ができるかどうかにも依存する。残念ながら、あまた存在する脅威主体が取りうる攻撃手口のすべてを広く把握してかつ深く理解している一人の人間(実施者)は存在しない。そのため、最近のセキュリティ監査の結果には、「漏れ・抜け」が必ず存在することを念頭に置く必要がある。

さらに、そのような「漏れ・抜け」の少ない監査結果があったとしても、読み手の知識不足や想像力の欠如などにより、発生可能性を低く見積るケースや、読み手の独自の判断で受け入れることを拒否するケースもある。そのため、十分な説明責任の構築ができず、セキュリティ対策に必要なリソースや予算獲得に至らない。結果として、実際の脅威に適合しないセキュリティ対策に留まり、脅威主体によるサイバー攻撃を許してしまう。

このような問題に対する解決策は、セキュテリィ監査の実施者及び読み手が、最近のサイバー攻撃の発生状況と自組織内の IT インフラの仕組みやプロセスを注意深く観察して理解を深めていくしかない。特に、攻撃手口の把握と理解に努めながら、セキュテリィ監査で得られる潜在的なリスクを取りこぼさないよう、洞察と想像力を鍛えていくことで、セキュリティ監査の読み取り方や説明責任の適正化につなげることができる。

おわりに

これまでのセキュリティ監査は、組織の IT インフラを守ることに偏重したものが多かったが、国全体のデジタル化が加速しつつある中で(確実に)発生するサイバーリスクにより、自組織だけでなく隣接する組織や顧客に対して被害を及ぼす可能性が高くなる。今年(執筆時点 2020 年 9 月まで)の国内のサイバーリスクに起因する事例を眺めると、すでに顧客に対する深刻な被害が相次いで発生している。

しかし、コロナ禍による厳しい財政状況の中で、すべてを網羅したセキュリティ対策を強化することは困難である。よって限られたリソースと予算の中で、最大限の効果を発揮するセキュリティ対策を組織全体として行う必要があり、そのためにはセキュリティ対策の説明を、合意形成による参加型意思決定をベースとした日本企業の現状に合ったものにしなければならない。特に、組織のセキュリティ対策を強くリードできる CISO 人材は僅かであり、既存の日本企業の文化慣習に受け入れられるまでには長い時間がかかるとみられる。

今後、日本企業におけるセキュリティ対策の適正化を図るためには、意思決定層の合意形成に影響を与えることが最善策である。そのために、セキュリティ監査の読み取り方や説明責任の構築を強化していくことで、意思決定層の困惑や迷いを避けつつ、組織全体のセキュリティ対策を向上させる機運を高めることにもつながる。

(了)