IIA Bulletin

The Institute of Internal Auditors

現在の最緊急課題に関する内部監査人の視点

2020年4月

パンデミック：ITの障害について考慮すべきこと

新型コロナウイルス感染症（COVID-19）のパンデミックにより、経済界は業務を行う上で想定外の対策を**余儀なくされ**、その結果、独特のリスクが発生している。これは特にサイバーリスクについて言える。ソーシャル・ディスタンシングや在宅要請に関連して業務の変更が続くことは明らかであり、在宅勤務、ビデオ会議の利用拡大、および付随するトラブル解決のためにIT資源が再配分されている。IT専門家はこれらの新たな要求に対処することを中心に業務を行っているので、組織体は新たなサイバー脅威や脆弱性に曝される可能性があり、さらに困ったことに、既存の脅威に注意を向けられなくなる可能性もある。

最も厄介なのは、「ゼロデイ」攻撃のリスクである。ゼロデイ攻撃とは、特定のソフトウェア、ファームウェア、機器構成、またはオペレーティング・システムの弱点に対して、開発者が気付いておらず望ましい対策がない段階で起こるサイバー攻撃である。このようなセキュリティの弱点、すなわち脆弱性は、プログラミング・エラー、または不適切なコンピュータやセキュリティの設定からしばしば起こる、未知または予想外の結果である。脅威は2つある。サイバー犯罪者はパッチが利用可能になるまでの短期間、この脆弱性を攻撃することが可能だが、望ましい対策やパッチが利用可能になり次第実装されなければ、この脆弱性は長期的な脅威となる。

内部監査人が現時点で実施できる重要な作業の1つは、パンデミックがITの資源、優先順位、および重点事項に与える影響を全面的に評価することである。その作業には、ITを最新の状態に維持し、ゼロデイ攻撃の可能性や他の脆弱性に気付くために、現行の手順が十分かつ効果的かを判断することを含めるべきである。

新型コロナウイルス感染症危機時にサイバー脆弱性を評価するための一般的な質問

1. 組織体は、ゼロデイ攻撃の可能性に関して、信頼できる報道機関や他の情報源をどのようにモニターしているか。これらのリスクへの対応プロセスは変更されているか。
2. 組織体は、必要なセキュリティ関連パッチがタイムリーに実装されているかをどのように確認しているか。
3. 組織体のプロセスや業務環境の変化により、スレットハンティング（積極的なサイバー防衛活動）や他のモニタリング活動とスキャン活動は変更されていないか。その結果生じるリスクには、どのように対処しているか。
4. 組織体は、業務環境の変化を受けて、脆弱性を管理する業務が適切に行われているかをどのように確認しているか。具体的には、どのような脆弱性スキャンや対策が変更または延期されているか。

5. 組織体は、ITインシデントを管理する業務（インシデントの防止、検知、対応の手順を含む）が最新の脅威に対応しているかをどのように確認しているか。IT部門は、現在のプロセスがイベントのトリアージ、分析、抑制、根絶、および対応に必要なツールとサービスを含んでいるかを、どのように確認し続けているか。
6. 組織体は、ネットワークの変更が適切に要求され、文書化され、承認され、実行されているかを、どのように確認しているか。これには特に、リモート操作を容易にするための緊急または臨時の変更が含まれる。
7. 組織体が物理的・論理的アクセスを許可するプロセスは、どのように変更されているか。業務環境の変化によって、アクセス権の追加、移転、終了のレビューや許可プロセスは延期されているか。
8. リモート業務環境では実行やモニターができない重要なプロセスはどれか。その結果生じるリスクには、どのように対処しているか。
9. パンデミックへ対応することによって、主要なクラウドベンダーとの関係を含むベンダーとの関係管理はどのように変わったか。
10. 契約管理に関して、どのような変更が行われたか。例えば、契約要件は、緩和または変更されているか。
11. 業務環境の変化に伴って、調達プロセスはどのように変更されているか。具体的には、ユーザが取得又は実施するシステム、アプリケーション、およびサービスが増加する可能性に対応するために、組織体は何を行っているか。

IIAの資源

Practice Guides

- GTAG: Business Continuity Management
- Practice Guide: Business Continuity Management
- GTAG: Assessing Cybersecurity Risks
- Practice Guide: Assessing the Risk Mangement Process
- Practice Guide: Auditing Third-Party Risk MAnagememt
- GTAG: Insider Threats

Training on Demand

- Auditing Insider Threats OnDemand

出典：内部監査人協会 “IIA Bulletin – Pandemics: Considerations for IT Disruptions”
https://global.theiia.org/knowledge/Public%20Documents/IIA-Bulletin-Pandemics-Considerations-for-IT-Disruptions.pdf