Deloitte.
デロイト トーマツ

トーマツ.

新型コロナウィルスがビジネスに与えるインパクトと対応

「リモートワークを進める上でのセキュリティ強化のポイント」

インドネシアにおいても新型コロナウィルスの感染が拡大し、事業継続に影響を与える事態となり、在インドネシア日系企業でも緊急事態への対応を余儀なくされています。多くの企業では、過去に整備されたBCP(事業継続計画)や感染が先行した中国・タイなどの他拠点での対応事例を基に、緊急事態への対応を講じています。一方、不透明な状況によって生じる経済・事業運営・サプライチェーンへの影響の長期化に対する備えは必ずしも十分とは言えません。有事対応の長期化を見据えて、柔軟性を高めて臨機応変に対応できる組織力を高めていく必要があります。

本稿では、リモートワークの導入・長期化を見据えた際のセキュリティ上の課題と対応策を解説します。

リモートワークは企業内の感染拡大リスクの低減策として有効な対策である一方、オペレーション、重要データの取り扱いや社内ネットワークの管理を複雑にし、情報セキュリティに係るリスクを高めます。たとえば、リモートワークとなった従業員が社外から社内ネットワークにアクセス可能とする環境を整えるケースでは、データへのアクセス権限を広範に開放するという対応とあわせて、データ漏洩リスクへの対応も合わせて検討が必要となります。業務効率と情報セキュリティのバランスを取りながら、すばやく対応していくことが求められます。

リモートワークの導入により、情報セキュリティの前提条件が大きく変わるため、以下の点を見直す必要があります。

(A)　ID管理・ユーザーアクセス管理の強化

＜リスク＞

リモートワークにおいては、ユーザーが業務を進める上で社内ネットワークにリモートアクセスを行う必要があります。そのため、ユーザーのアクセス権限の見直しやアクティビティのモニタリング強化が必要となりますが、権限を越えたアクセスや機密情報のダウンロード・変更・削除などの不正アクセス・不正処理による重要データの喪失・漏洩などのリスクが伴います。

強化

＜対応のポイント＞

まず、アクセス権限の設定方法やリモート接続の見直し・データ管理ルールなどの情報セキュリティ基盤をより強固なものにする必要があります。その上で、不正アクセスや不正処理の早期発見のためのモニタリングを徹底することが重要です。対応策例は以下の通りです。

■ 情報セキュリティ基盤の強化方法（例）

- 社外でのデータの取扱ルールの整備
- 重要な情報資産へのリモートアクセスの可否の決定
- リモートアクセスを行うユーザーの接続方式の見直し・制限（VPN接続、多要素認証、2段階認証方式の導入など）
- ユーザーIDの棚卸・付与権限の精査
- 権限設定承認プロセスの厳格化
- パスワード設定ルールの厳格化（有効期間の短縮、強度の高いパスワード要件の設定など）

■ モニタリングすべき事項（例）

- ユーザーアクセス（ID、付与権限、付与期間、アクセス内容、頻度、アクセス方式、操作内容など）
  - 職務範囲とは関係ないと思われるIDはないか？
  - 異なる方式・ポイントで、頻繁にログインしているIDはないか？
  - パスワードの入力誤りなど頻繁にログインを失敗しているIDはないか？
    ※不正アクセス検知のため

- ユーザーのアクティビティ・データ処理
  - 大量にデータをダウンロードしていないか？
  - USBメモリなど禁止されている場所に機密データを保存していないか？
  - 重要なデータの変更・削除などのログを記録できるようになっているか？

(B)　ネットワークとアプリケーション管理の強化

＜リスク＞

リモートワークは通常のオフィス環境とは異なり、家庭用Wi-Fiやモバイル端末のローミングなどの多様な接続手段を利用されることが想定されます。必ずしも信頼できるネットワークではないため、データを盗み取られるなどリスクが高まります。また、以前より問題となっていますが、チャットアプリやオンラインストレージを利用した機密情報のやり取りが増加することが想定されます。

＜対応のポイント＞

公共Wi-Fiなど信頼性が不確かなネットワークへの接続を禁止するとともに、データ通信の暗号化を施すことが必要です。また、定期的に自社のセキュリティの脆弱性の評価や侵入テストなどを実施し、適時に改善・補強していくことも重要です。

加えて、会社が許可していないメールサービスやチャットアプリの利用時の注意事項など機密情報の取り扱いについてガイドラインを作成し、従業員に周知することが必要です。自社のIT環境では業務が進めにくいという「不満」・「不便」が、外部サービスの利用につながっているため、ユーザーのニーズを把握することも重要です。安全性の高い代替サービスの提供などリモートワークという環境においてユーザーが業務を効率的に進められるインフラ整備に取り掛かるべきです。

(C)　セキュリティ・インシデント対応態勢の強化

＜リスク＞

通常とは異なる勤務形態に移行することにより、ネットワーク環境・端末などのハード面・従業員の意識などソフト面も変わるため、情報漏洩・誤操作などのインシデントの発生可能性は高まります。

＜対応のポイント＞

予防・早期発見に向けた取り組みだけでなく、従業員による情報持ち出しや外部からのアタックによる情報漏洩などのケース毎にインシデント対応手順を事前に策定しておくことが必要です。インシデント対応手順として、発生時の連絡手順（連絡先、連絡方法など）を明確化し、従業員への周知徹底を図ることも必要です。また、応急措置の決定プロセスや本社・関連当局への報告ルートも事前に確認しておくことが望ましいです。

(D)　従業員への継続的な注意喚起

＜リスク＞

残念ながら、危機・混乱に乗じた悪意ある者によるサイバー攻撃を受け、機密情報が流出するなどの被害が確認されています。ランサムウェアなどのマルウェアによる攻撃だけでなく、ビジネスメール詐欺(*1)に代表されるソーシャルエンジニアリング(*2)による被害も発生しています。

*1 ビジネスメール詐欺

取引先や自社の経営者等になりすまして、従業員をだまして送金取引などに係る資金を詐取するなどの金銭的な被害をもたらすサイバー攻撃

*2 ソーシャルエンジニアリング

ネットワークに侵入するために必要となるパスワードなどの重要な情報を、情報通信技術を使用せずに盗み出す手法全般

＜対応のポイント＞

一般的に、情報セキュリティにおいて一番の弱点は人間だと言われています。最先端のテクノロジーで強固なセキュリティシステムを構築しただけでは、人間の不注意などの脆弱性を突いた手法によるサイバー攻撃を回避することは困難です。対策としては従業員への注意喚起が重要となりますが、リモートワークではコミュニケーション手段が限定されるため、より一層の工夫が必要です。メールだけでなく、部門・チーム単位で実施される定例の電話会議などで被害事例を共有するなど繰り返し注意喚起を行い、従業員のセキュリティ意識を高めることが求められます。

上記(A)・(B)について、社内リソースでのモニタリングが難しい場合には、サイバー監視センターのような外部専門機関を利用し、不正アクセスの有無などを監視することも有用です。

【リモートワーク環境でのセキュリティを確保するために最低限押さえておきたいポイント】

確認事項		
1.	情報セキュリティ 態勢(ルール/組織)	☐ 情報セキュリティに関する基本的な規程が整備されており、リモートワーク実施に関するルール(社外でのデータの取り扱い等)が明記されている。
		☐ 情報セキュリティ対策に関わる体制(責任者/担当者)が定められている。責任者・担当者がリモートワークを行う場合、連絡方法・連絡先が明確になっている。
		☐ 重要な情報資産を特定し、リモートワークによる利用の可否を定めている。利用可能なデータの取り扱い方法が定められている。
		☐ 要員確保・問い合わせ先の周知徹底・FAQの整備などヘルプデスクのサービス品質維持のための施策が行われている。
2.	アクセス管理・物理的セキュリティの状況	☐ 重要な情報・システムに対するアクセス権限が設定されており、必要な従業員にのみ権限が付与されている。
		☐ アクセス権限の変更に関する承認プロセスが定められている。
		☐ 定期的にユーザーIDの棚卸・付与権限の精査を行っている。
		☐ リモートアクセスを行うユーザーの接続方式の見直しを行い、VPN接続、多要素認証、2段階認証方式などのより強化な方式を導入している。
		☐ パスワード設定・変更に関するルールが定められ、実装されている。
		☐ ログ管理などユーザーのアクティビティがモニタリングできるようになっている。また、定期的にモニタリングを行っている。
3.	情報セキュリティ・ネットワークの運用管理状況	☐ 自社のセキュリティに関する脆弱性診断やペネトレーションテストを定期的に実施している。
		☐ マルウェアの検知やマルウェア対策に関するルールが定められ、運用されている。
4.	インシデント対応	☐ 情報漏洩・システム障害等のインシデント発生時の報告ルート・対応手順が定められ、従業員に周知されている。
5.	従業員への継続的な啓発・注意喚起	☐ 従業員の情報セキュリティの重要性を理解させるための研修・教育を行っている。
		☐ リモートワークにおける留意点・注意喚起のための施策(メールの展開など)が検討・実施されている。

COVID-19は日系企業の皆様に限らず誰も経験したことのない事態であり、Deloitteリスクアドバイザリーは「経済社会のカタリスト」でありたいというデロイト トーマツ グループのビジョンに基づき、この事態を変革によって勝ち抜くための情報提供を継続して参ります。皆様のお声をぜひお聞かせください。蓑和を中心にDeloitte一丸で取組んでまいります。
よろしくお願いいたします。

柳澤　良文（東南アジア責任者）

デロイトインドネシアのリスクアドバイザリーチームは、リスク管理や業務改善に関する知見やサービスの提供を通じて、困難に直面されている在インドネシア日系企業と共に難局を乗り越えていけるよう精一杯尽力する所存でございます。危機対応や業務再開に向けてお困りのことがございましたら、いつでもお気軽にお問い合わせくださいませ。

蓑和　秀夫 (インドネシア責任者)

※貴社および貴社の関係会社とデロイト トーマツ グループの関係において監査人としての独立性が要求される場合、本サービス内容がご提供できない可能性があります。詳細はお問合せください。

本件に関するお問い合わせ先
Mail ap_risk@tohmatsu.co.jp

IS 669126 / ISO 27001