第16期企業ガバナンス　第２回セミナー　講演要旨

「情報セキュリティとコーポレートガバナンス」
～インシデント事例を通じて-～

- 日　時：2021年５月31日（月）14：30～16：30
- 場　所：Zoomを利用したオンライン方式 スタジオ651より配信
- テーマ：「情報セキュリティとコーポレートガバナンス～インシデント事例を通じて」
- 講　師：株式会社ラック サイバーセキュリティサービス統括部長 内田法道氏
- 参加者：39名（含、後日録画視聴者）

講演要旨

まず内田氏の経歴やLACのサービス内容が簡単に紹介された後、以下の主旨内容にて講演が行われた。

1. 最近のインシデントの状況について

- LACにくる相談は年平均すると300~400件で、最近はマルウエア系がほぼ50%。特に身代金要求型であるランサムウエアが近年増加している。システム開発委託先の社員によるソースコードの持ち出しや、自社社員による営業機密情報の持ち出しなど内部犯も８％ほどあるが、統計に表れる以上に実態はもう少し多いとみている。
- LACと契約に至らなかったが、当初インシデントの相談を受けた企業として、近年中小企業等の割合が50%を超えるなど拡大傾向にある。コストが理由で契約を見送ったと見られるが、取引先等に大企業を持つものもあり、対策が中途半端になっていないか懸念している。
- コロナ禍の影響でリモート勤務が増えたことで、急ごしらえのシステム上の脆弱性を狙った攻撃も増えている。
- 攻撃の目的はほとんど金銭目的が多いが、外国の政府や軍による機密情報の窃取などを目的とした標的型攻撃も常に一定数ある。
- 攻撃側の金銭要求には応じないことが基本。但し、例外的に人命が掛かっている病院システムのケースなどでは、要求に応じることもあるようだ。

- ランサムウエア被害の原因としては、VPN機器の修正プログラムが未適用や、安易なパスワードの設定・使用などがあり、定期点検を怠らないことが重要だ。

2. インシデント対応時の方針について（事例を交えて説明）

- 経営者は経産省策定のサイバーセキュリティ・ガイドライン（2017年版）を参照すると良い。
- インシデントが発生したら、①原因追求よりまず被害の拡大を防ぐ　②デジタル情報は消えると認識し、証拠データの保全に努める　③影響を狭く考えず、風呂敷を広げて検証しながら徐々に絞り込んでいく。決め打ちはしない。　の３つの原則を意識し行動すると良い。
- 往々にして、確証がないからと公表を躊躇したり、担当社員個人の責任追及をしたりしがちになるが、これらはインシデント発生時に最もやってはいけないことだ。叱責により当該社員が退社すれば復旧にも多大な影響が出る。

3. 今後のセキュリティ対策動向について

－ 今後注目されると思われるセキュリティ対策

- ゼロトラスト － never trust, always verify
  クラウド利用が拡大し、システム上の社内と社外の区分が曖昧になってきていることから、社内システムだからと安心せず常に検証を怠らないようにしよう。
- XDR － crossover detection & response
  エンドポイント、ネットワーク、クラウドからバランスよくデータを集め、マルウエアの侵入を面で防ごうとする機械学習エンジンが最近注目される。
- シフトレフト
  「抑止」→「防止」→「検知」→「復旧」の順番では、より手前での対処が効率的であるという考え方。従来はシフトライトとして最後段階の「復旧」にまず重点が置かれていた。
  コスト面では早期対応がやはり有利となる。

4. 終わりに

- 自社の意外な価値は攻撃者が知っている。攻撃者の視点で考えると良い。
- 攻撃する側は金銭目的が多い。他社比較でより脆弱な組織が狙われる。他社に劣後しないようプラスαの対策を怠らないこと。
- 継続的な対策や多層防御が重要。
- 完全無欠なシステムは無いと自覚し、臨機応変な対応ができるように常日常心がける。

以上