情報システムペネトレーションテスト エクスプレス事例

株式会社光電製作所 様

光電製作所は、電子技術の先駆者であった海軍技術研究所を前身とし、航海や漁業を支える船舶用電子機器のリーディングカンパニーとして発展してきた。船舶の安全運航を支える同社は、「電波」「音波」「光波」を活用して高精度な位置情報を取得する「センシング技術」と、情報を安全・確実に保護・伝送する「情報保護技術」を強みとしている。「技術のコーデン “Sensing for your dream.”」を掲げ、社会の安全・安心を支えてきた同社にとって、「安全性」は業務環境の安全性に留まらず、事業そのものの信頼を支える重要な要素として位置付けられている。

こうした考えのもと、光電製作所の情報システム部では、製造にかかわるシステムを担当する DX 課と、社内のシステム、社内ネットワークの維持・管理を行う情報システム課が連携し、セキュリティ強化に取り組んでいる。今回は、ペネトレーションテストを依頼した情報システム課の坂口 徹氏、竹川 和也氏に話を伺った。

「対策しているつもり」と「実際に防げるか」のギャップ

光電製作所は、セキュリティ対策の重要性を早くから認識し、継続的な取り組みを進めてきた。ラックの監視サービスや、ラックセキュリティアカデミーの研修も活用しており、決して「対策が不十分な企業」ではなく、組織的かつ継続的なセキュリティ対策を講じている企業である。

情報システム課 課長 坂口 徹氏

一方で、サイバー攻撃が高度化する中、「対策を導入していること」と「実際に攻撃を防げること」は必ずしも一致しない。光電製作所では、社内ネットワークの更改を見据え、現行環境に潜在的な問題がないかを客観的に評価するため、外部サービスによる診断の実施を検討していた。社内にも専門知識を持つ人材はいるものの、限られたリソースの中では「自分たちだけでは十分に対応しきれない領域は外部を活用する」という考えを以前から持っていた。

そのような中、ラック主催のイベントで「情報システムペネトレーションテスト エクスプレス」を知り、「情報システムに実際に侵入テストを行う」という説明に強い関心を抱いた。「自社の対策は本当に有効なのか」、「実際に攻撃された場合にどこまで侵入されるのか」という疑問から、机上のリスク評価ではなく、実際の攻撃シナリオに基づいて防御力を検証したいと考えた。

導入の決め手と社内合意形成

今回のペネトレーションテストでは、侵入後にどこまで影響が拡大するかを中心に設計された。対策の有無を確認するだけでなく、実際の攻撃を想定した際の影響範囲を把握することに重点を置いたのだ。

印象的だったのは、ペネトレーションテスト実施に向けた経営層の意思決定の速さだ。坂口氏は、「社長自身が過去のネットワーク構築に関与していたこともあり、リスクを客観的に把握することの重要性を深く理解しており、速やかに実施への合意が得られました。」と語る。自分が関わったから信じるのではなく、関わったからこそ改めて安全性を検証したいという姿勢は、情報システム課のセキュリティ意識の高さにつながっている。

また、社員全体として「特別にセキュリティ意識が高いわけではない」としながらも、不審なメールを受信した際には、気づいたことをすぐ共有できる文化が根付いているという。インシデント対応において、こうした心理的安全性の高い組織風土は、早期発見・早期対応を支える重要な基盤となる。

一方で、ペネトレーションテストの実施範囲をどこまで広げるべきかについては、社内で活発な議論が交わされた。経営層から「ここは対象外としてほしい」といった意見が出る場面もあり、情報システム課の要望と事業上の懸念のバランスを取りながら、ラックもテストの目的や意義を説明し、範囲の調整を進めた。このプロセスは事前調整にとどまらず、組織として何を守るべきかを改めて議論する機会となり、重要資産や事業継続の観点から優先順位を再確認できたことは、ペネトレーションテストがもたらした大きな副次的効果だった。

検証結果と得られた示唆

テスト結果のレポートについて竹川氏は、「専門家でない担当者でも理解しやすい内容でした。技術的な詳細だけでなく、経営判断に必要な要点が整理されており、そのまま社長への報告資料として活用できました。」と高く評価した。ラックとしても、ペネトレーションテストは実施して終わりではなく、経営層がリスクを理解し、次の判断につなげるところまでがレポートの役割と考えており、その点をご評価いただけたことは大きな成果だった。

さらに、終了後すぐに「ネットワーク更改後にも実施したい」という声が上がっている。一度きりのペネトレーションテストではなく、システ

ムや事業環境の変化に合わせて継続的に検証を行う重要性を実感されたようだ。さらに、検証範囲の検討過程そのものが、「何を守るべきか」「どのリスクに優先的に対応すべきか」を経営層が主体的に考えるきっかけにもなった。光電製作所では、セキュリティはコストではなく事業継続の前提条件という考え方が定着し、組織全体でセキュリティと向き合う文化をさらに強化する機会となった。

情報システム課 竹川 和也氏

どのような企業に有効か

インタビューの最後に、「このようなサービスは、どのような企業に適しているか？」を尋ねたところ、「ネットワークにつながっているのであれば、すべての企業がやるべきだ。」とコメントをいただいた。

特に、「自社は大丈夫と考えている企業ほど、潜在的なリスクを見落としやすい」という指摘があった。また、中小規模の企業では日々の業務に追われ、脆弱性の把握や対策の優先順位付けまで手が回らないケースも少なくない。さらに、「ひとり情シス」のように限られた人員で運用を担う企業では、改善対応の負荷が課題になることもある。しかし、だからこそ第三者の視点で現状を客観的に可視化する価値があるという。「自社は大丈夫」と思ったその瞬間こそ、客観的な検証が必要なのかもしれない。今回いただいた言葉は、ラックがお客様にペネトレーションテストの価値を伝えるうえで重要なメッセージとなった。

ペネトレーションテストの本質的な価値

今回の取り組みから見えてきたのは、ペネトレーションテストが持つ実践的な価値だ。ラックでは、ペネトレーションテストを「現実的な攻撃シナリオを用いて攻撃耐性を確認する」診断と位置付けている。システムへの侵入につながる脆弱性の発見自体が目的ではなく、攻撃者がどのような経路や方法で目的を達成し得るのかを明らかにするための取り組みである。

重要なのは、「何が危険か」を指摘することではなく、「何を守るべきか」「どのリスクに優先的に対応すべきか」を組織全体で共有することにある。実際の攻撃を想定した検証は、現場だけでなく経営層にも具体的な危機感をもたらし、セキュリティを共通言語として議論するきっかけとなる。今回の取り組みは、ペネトレーションテストが経営と現場をつなぐコミュニケーションの契機にもなり得ることを示した。

また、すでに一定の対策を講じている企業であっても、実戦的なシナリオに基づく検証を通じて新たな気づきを得られる。何より、対策の有無を確認するだけでは見えてこないリスクも、実際に攻撃してみることで初めて明らかになることがある。「自社は十分に対策できている」と考えている企業ほど、一度立ち止まり、現実的な攻撃シナリオで自社の防御力を確かめてみる価値があるのではないだろうか。

左から、情報システム課の坂口 徹氏と竹川 和也氏

［お問い合わせ］
株式会社ラック
サービス紹介ページ　https://www.lac.co.jp/consulting/exp_penetration_test.html