概要

日本サイバーディフェンス（NCD）では、サイバー攻撃、特にランサムウェアの攻撃がもたらす影響を観察してきました。大規模なランサムウェアの攻撃が新聞の見出しを飾ったこともありましたが、実際には非常に多くの組織が影響を受けています。

このような攻撃の数と巧妙さの増加は、RaaS（Ransomware as a Service）によって、洗練されたサイバーツールがますます多くの犯罪グループに利用されるようになったことに起因しています。

NCD アドバイスサービスの唯一の目的は、サイバー攻撃からの回復を支援することです。

製品とサービス

ランサムウェアの評価: NCD は、ランサムウェアの全体的な影響と深刻度の評価をします。全体的評価が行われた後、組織は次のステップについてアドバイスを受けます。

ランサムウェアのインシデント対応: NCD は、インシデントをどのように管理するか、詳細なプランを提供します。高度な専門知識を持つアドバイザー集団が、最善の方法でインシデントに取り組むことを支援します。

恐喝の交渉: NCD は、組織へのサービスとして、恐喝交渉と脅威行為者との必要なコミュニケーションを提供します。NCD は、脅威行為者から必要な情報をすべて取得し、インシデント全体を責任を持って処理します。

決済・復号化対応: NCD は、ランサムウェアの攻撃で暗号化されたファイルの復号化に必要なあらゆるサポートを提供します。また、脅威行為者とのコミュニケーションに基づいた決済サービスを提供します。

ランサムウェア・暗号フォレンジック: 当社の暗号ランサムウェアのフォレンジックサービスの目的は、お客様の crypto 取引、取引間で転送されるアドレス、ウォレット、さらに取引、アドレス、ウォレット、取引に関与する者の関係を詳細に洞察することです。

インシデント・レスポンス・リテーナー: NCD は、組織にとっての保険のような役割を果たすリテーナー・サービスを提供しています。リテイナー・サービスは、適切なインシデント対応、詳細なレポート分析、インシデント発生時の完全なサポート、暗号通貨の決済と復号化のサポート、恐喝交渉、詳細なインシデント対応、所定の SLA 内での復旧レポートなどのサービスを組み合わせて提供します。また、組織は NCD からの警告と調査の完全なアクセスを提供されます。

追加サービス: この追加サービスは、上記で定義されたすべてのサービスに付随しており、以下の内容を含みます。

- サイバーインシデントの前後での技術的ソリューションの開発と展開
- 会社内部の認識向上、インシデント計画と演習

インシデント種類

以下のようなインシデントタイプを扱っています。

- ランサムウェア
- 脅威となる人物がデータファイルを暗号化すること。
- データ漏洩の脅威.
- アカウントやデータの漏洩

手順

サービスの仕組み

- サイバー攻撃の被害に遭ったと思われる企業の方は、NCD のオンラインポータルからご連絡ください（攻撃で漏洩した可能性のあるメールアドレスは使用しないでください）。

- 機密保持のための NDA（機密保持契約）

日本語を母国語とする担当者との最初の話し合いの後、企業の経営陣と、何百ものサイバー・セキュリティ・インシデントに対処してきた世界トップク

ラスのサイバー・セキュリティ専門家との間で、安全なビデオ会議通話が設定されます。この通話は、英語または日本語の通訳付きで行うことができます。

シニアマネージャー（CEO、CIO、CFO、CISO など、サイバーインシデント管理のリーダー等）が、専門家に質問する機会が設けられています。質問の内容は、ベスト・プラクティスやプアー・プラクティスに関する一般的なものから、特定の技術的なものまで様々です。