2022 年 10 月 12 日

セキュリティ連盟

『サイバー犯罪から顧客情報を守る！ Web サイト上で個人情報を取得する企業が気を付けるべきこと』セミナーを実施しました

セキュリティ連盟は深刻な社会問題であるサイバー攻撃への「対策の重要性」を啓発するべく、2022 年 8 月 25 日（木）に EC 事業者を中心に『サイバー犯罪から顧客情報を守る！ Web サイト上で個人情報を取得する企業が気を付けるべきこと』セミナーを開催いたしました。

当日はセキュリティ連盟の起案企業である株式会社サイバーセキュリティクラウド 代表取締役社長 兼 CEO 小池敏弘氏のご挨拶から始まり、警察庁 サイバー警察局 サイバー企画課の津村佳孝氏からは「サイバー犯罪の概況」についてお話しいただきました。

続いて、アイレット株式会社 クラウドインテグレーション事業部 セキュリティセクション 特命グループ グループリーダー 中村 昌登氏から「クラウドで始める EC サイト構築のメリットと落とし穴」についてご講演いただき、フィッシング対策協議会 平塚伸世氏からは「フィッシング詐欺の実態・対応策」についてお話しいただきました。

その後は、一般財団法人日本サイバー犯罪対策センター 大野克巳氏と、明治大学 サイバーセキュリティ研究所 所長 齋藤孝道氏、株式会社サイバーセキュリティクラウド 経営企画部 技術広報 中山貴禎氏にご登壇いただき「Web スキミングの実態・対応策 悪質ショップサイトへの誘導に関する実態・対応策」について、トークセッション形式で語っていただきました。

【お問い合わせ先】
セキュリティ連盟事務局：竹谷
E-mail：pr@cscloud.co.jp

日本の DX をもっと安全に

セミナーの後半では、三菱 UFJ ニコス株式会社 加盟店管理部 次長 吉岡徳氏から「『個人情報漏洩』『不正利用』に関する事例・対応」をお話しいただき、株式会社リンク セキュリティプラットフォーム事業部 事業部長 滝村享嗣氏からは「クレジットカード情報漏洩時の被害インパクトと対策」についてお話しいただきました。

セキュリティ連盟は今後も、本アクションの様々な取り組みを通じてサイバーセキュリティ対策の重要性を啓発するべく尽力してまいります。

■「サイバー犯罪の概況」について
警察庁 サイバー警察局 サイバー企画課 津村 佳孝 氏

現在、情報通信技術の発展や、デジタル化の進展によって、サイバー空間は重要な社会経済活動が営まれる公共空間へと進化しており、社会全体のサイバーセキュリティ対策を向上させることが重要となってきています。また昨今、新型コロナウイルスの影響で企業活動や生活が変化しており、本人確認方法なども変わってきております。

様々な社会経済活動がサイバー空間を通じて非対面や非接触で行われるものへと大きく移行する中、サイバー空間における脅威は極めて深刻な情勢が続いております。更にこれまでのサイバー空間は、それ相応のリテラシーを持った方が利用する空間でありましたが、今では誰もが利用する空間になっています。

このような情勢を踏まえて警察庁では、2022 年 4 月に組織改正を行い、警察におけるサイバー戦略を掲げ警察組織の総合力を発揮して効果的な対策を推進しています。

全国警察が一体となって対策を推進する一方で、警察のみの力では対応が出来ません。全ての企業・団体がサイバーセキュリティ全体の底上げに向けて、多様な主体との連携が必要となってきます。特に、サイバー犯罪の被害拡大や再発防止には、被害を潜在化させないことが重要であるため、もし攻撃を受けたら速やかに警察への通報をしていただきたいと思います。

■「フィッシング詐欺の実態・対応策」について
フィッシング対策協議会 平塚 伸世 氏

フィッシング報告件数について、ここ 2～3 年で非常に大きな問題となってきました。2020 年以降急激に伸びており、2019 年と比較すると、すでに 10 倍の報告数となっています。さらにフィッシング URL 件数につきましても、2022 年 7 月度に過去最高の 10 万件を観測しており、その時点において 2019 年の約 6.4 倍と増加しています。これらに対抗する為にはフィッシングメールへの対策が重要となります。

フィッシング対策協議会では、フィッシング対策ガイドラインを公開しております。フィッシングは世の中の状況に合わせて常に変化している為、毎年、改定しています。一度、狙われると対策がなされるまで狙われ続けることになるので、ご注意下さい。特にクレジットカードなどの利用が出来る Web サイトは規模に関係無くフィッシングで狙われる可能性が有ります。

フィッシング対策ガイドライン 重要 5 項目
1）利用者に送信するメールには「なりすましメール対策」を施すこと
2）複数要素認証を要求すること
3）ドメインは自己ブランドとして認識して管理し利用者に周知すること
4）全てのページにサーバ証明書を導入すること
5）フィッシング詐欺について利用者に注意喚起すること

■ トークセッション
「Web スキミングの実態・対応策 悪質ショップサイトへの誘導に関する実態・対応策」

【お問い合わせ先】
セキュリティ連盟事務局：竹谷
E-mail：pr@cscloud.co.jp

一般財団法人日本サイバー犯罪対策センター　大野 克巳 氏

攻撃者側のモチベーションは何かと想像すると、金銭的な目的が一番かと思います。
フィッシング詐欺については企業のブランドを語って ID／パスワードの情報を盗取するので、そういった意味でいうと、国内企業様は幅広くターゲットになりえます。
フィッシングサイトはクレジットカード情報を入力させる画面に遷移させる場合がほとんどです。利用者が全く気付かない Web サイトの改竄（Web スキミング）なども存在します。クレジットカードや個人情報が盗まれてしまうと、その情報自体を販売したりと、盗んだ側が自由に使えてしまうので、まずは盗まれない様にすることが重要になります。
リスクはいつでもあることを前提に、あらかじめ準備しておくことが重要だと思います。平素からインシデントが起きたときの対策をどうするかなどの準備が必要になります。

明治大学 サイバーセキュリティ研究所 所長　齋藤 孝道 氏

攻撃者もそれぞれ特徴（収益モデル・脅威モデル・犯罪モデル）を持っており、対象の業種・業態に応じて、マネタイズをしています。その為、攻撃者の特徴を理解して、自分自身の業種・業態にどの様なリスクが有るのかを把握し、その対策の準備することが重要です。
いざ攻撃を受けてしまうと、慌てて何もできなくなってしまうので、トレーニングをしっかりとしておいた方が良いと思います。経営者が本腰を入れないと、有効なセキュリティ対策は確立できず、いざインシデントがあると会社が傾いてしまうので、経営課題の一つにすべきだと思います。

■セミナー参加者の声（アンケート原文引用・一部抜粋）
・事例紹介等、大変参考になりました。今後もセミナーの機会をいただけましたら、拝聴したいと存じます。
・サイバーセキュリティ技術の進化、リスクマネジメント、ガバナンスへの取り組みについて聞いてみたいです。
・また興味を引くテーマでのセミナーの紹介をいただいた際には参加させていただきたいです。

■セキュリティ啓発アクション『日本の DX をもっと安全に』の活動内容
セキュリティ連盟は、サイバー攻撃による具体的な被害や、被害に遭った今だからこそお伝えが出来る実際に必要だった対応などの、これまであまり公開されることがなかった「サイバー攻撃被害の裏側」を具体的に生々しく共有する場を設けます。このアクションを通して、社会問題となっているサイバー攻撃への関心を喚起し「対岸の火事」では済まされない「セキュリティ意識の醸成」を図ります。

セキュリティ連盟への加盟、セキュリティ啓発アクション『日本の DX をもっと安全に』への賛同をご希望される方は、下記よりお問い合わせください。

★　加盟・賛同に関するお問い合わせ：pr@cscloud.co.jp　（セキュリティ連盟　事務局：株式会社サイバーセキュリティクラウド）
★　『日本の DX をもっと安全に』の特設サイト：https://www.cscloud.co.jp/dx-security

【お問い合わせ先】
セキュリティ連盟事務局：竹谷
E-mail：pr@cscloud.co.jp