【ニュースリリース】

2023 年 4 月 7 日

株式会社サイバーセキュリティクラウド

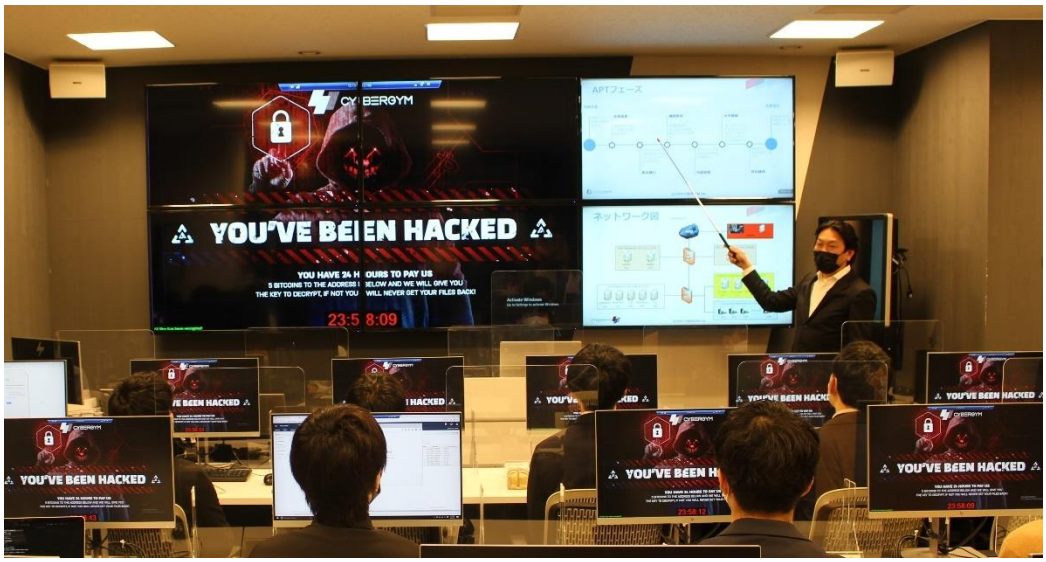
報道関係者各位

全 PC が乗っ取られる！
『体験型』サイバーセキュリティ研修を実施
～若手社員を対象に「サイバーセキュリティマインド」の向上を～

ハッカー対策サービスを展開するグローバルセキュリティメーカーの株式会社サイバーセキュリティクラウド（本社：東京都品川区、代表取締役社長 兼 CEO：小池 敏弘、以下「当社」）は、当社が発起人の一般社団法人サイバーセキュリティ連盟主催の「『体験型』サイバーセキュリティ研修」を 2023 年 4 月 4 日(火)に実施しました。

本研修は、最新の「サイバーセキュリティマインド」調査（※）で、一般クラス社員のサイバーセキュリティ意識の低さが判明したことを承けて、若手社員を中心とした一般クラス社員の「サイバーセキュリティマインド」向上を目的としました。

※「サイバーセキュリティマインド」調査（株式会社サイバーセキュリティクラウド 調べ）
https://prtimes.jp/main/html/rd/p/000000323.000009107.html

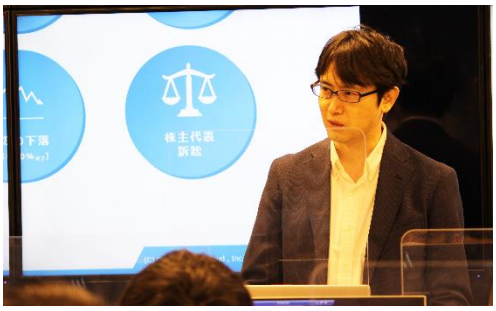


体験型サイバーセキュリティ研修は、座学だけでサイバーセキュリティについて学ぶのではなく、眼前の PC が実際にサイバー攻撃に遭う体験などを通じ、若手社員に危機意識を持ってもらうための内容となっています。研修には当連盟に入会している企業の若手社員：10 名が参加しました。

研修では当社の代表取締役 CTO 渡辺洋司の挨拶から始まり「昨今のサイバー攻撃概況」についてお話ししました。続いて、サイバーコマンド株式会社 代表取締役 兼 CEO 浦中究氏にご登壇いただき「サイバー攻撃の種別」についてお話しいただきました。

研修の後半にはサイバーコマンド株式会社 取締役 兼 CTO 横濱悠平氏にご登壇いただき「サイバー攻撃の実例」についてお話しいただいた後、受講者全員に眼前の PC で疑似ハッカーによるサイバー攻撃を受けていただき、サイバー攻撃への対応策を始め、サイバーセキュリティの大切さを体感していただきました。

■昨今のサイバー攻撃概況
株式会社サイバーセキュリティクラウド 代表取締役 CTO 渡辺洋司



インターネットの利用増加や企業の DX によりサイバー攻撃は年々増えております。企業におけるサイバー攻撃被害は、個人情報の流出だけでなく、売上機会の損失やブランドイメージの毀損、株価の下落など様々な影響があります。また、それだけでなくサイバー攻撃被害に遭った自分たちから情報が漏れることで、今度は加害者にまでなってしまうということがサイバー攻撃の怖さです。

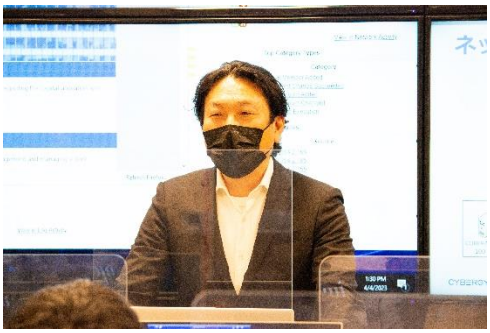
今や、サイバー攻撃は業種問わずに対策が必要となっています。この研修を通して少しでも多くの方がサイバーセキュリティ対策に目を向けていただけたらと思っています。

■サイバー攻撃の種類
サイバーコマンド株式会社　代表取締役 兼 CEO 浦中究氏

PC には様々な情報が格納されており、調べようと思えばかなり細かい部分まで情報を取ることが出来ます。サイバー攻撃は目に見えないことが多く、例えばファイルデータをコピーして抜き出されてしまうと PC 上や Web 上には原本データが残り続けているため、情報を抜かれたことにすら気づきません。またサイバー攻撃は 1 回やられて終わりと思う方が多いのですが、実は情報収集から始まり、長い時間をかけて潜伏し、万全な状態を築いてから情報を盗んでいきます。

今回の研修ではどのような流れでサイバー攻撃が行われていくのかを時系列で体験していただきたいと思います。

■サイバー攻撃の実例
サイバーコマンド株式会社　取締役 兼 CTO 横濱悠平氏

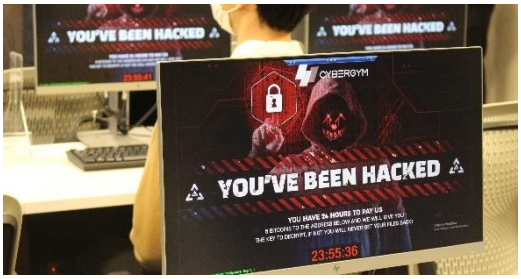


本来、標的型攻撃は 8 つの段階があり、最初は情報収集のためにアクセスをするところから始まります。この標的型攻撃は短期間で行われるものではなく、数ヶ月から 1 年程度の非常に長い期間の潜伏と情報収集をしています。

今回の研修では、標的型攻撃といった特定の組織に対して明確な目的を持ったサイバー攻撃や「サイバーキルチェーン」と呼ばれるサイバー攻撃対策の一連の流れなどを理解してもらうために短時間で分析をしながら進めていきます。

【報道関係者各位の問い合わせ先】
株式会社サイバーセキュリティクラウド　経営企画部　広報担当：竹谷・川﨑
TEL：03-6416-9996　Mobile：080-4583-2871(川﨑携帯)
FAX：03-6416-9997　E-Mail：pr@cscloud.co.jp

■サイバー攻撃実体験ブロック



今回はグローバルレベルの実践的サイバーセキュリティトレーニングを提供するサイバージムの環境を活用し、代表的な標的型攻撃をどのような兆候が表れるのか段階的に全体で確認しながら行っていきました。

受講者は PC 内に入っているログ収集（アクセス状況収集）ソフトを用いて、Web サイトへのサイバー攻撃を監視し、参加者全員がチームとなりシステムの防衛を試みました。

まずは監視システムで短時間に何回も機械的にアクセスされているポイントを検知し、そこでどんな状況が起きているのかを確認しながら進みました。次第に監視システムが段階的に異常を検知し、対象 Web サイトにアクセスすると別の Web サイトに強制的に飛ばされました。

そこからどんどんと新たな異常を感知し、ついには Web サイトの閲覧ができなくなりました。その後、わずか 30 分で参加者全員の PC がランサムウェアに感染し、PC を操作することができなくなりました。

受講者からは「サイバー攻撃は見えないからこそ怖い」「一瞬の出来事で何も出来ずにハッキングされてしまった」など、恐怖を覚える声が多くあり、参加された若手社員全員に危機感が芽生えたようでした。

■受講者の声

- クロスサイトスクリプティング（XSS）という単語を知っているなど、サイバー攻撃に関する知識は少しある方だと思っていたのですが、まさか PC が全く動かなくなるまでになるとは思っていなかったので、びっくりしました。Web サイトへの攻撃だとパスワードが抜かれる、個人情報が抜かれるくらいに思っていたため今までの認識が違ったことを痛感しました。研修に参加出来て良かったです。
- 最初はネットワークの構成図などを確認した際にはサイバーセキュリティもしっかりしていると思っていたのですが、実際に研修が始まったら、ものの 30 分くらいでハッキングされてしまうことに恐怖を感じました。画面にしっかりと出てくる異常には気づくことが出来ましたが、内部で行われていることには気づくことが出来ませんでした。
- サイバー攻撃は脆弱性や人為的ミスの積み重なりによって被害を大きくしてしまうと思っていたのですが、一つの Web サイトを開くだけで PC が動かなくなってしまう程だということにとても驚きました。研修を受けて、Web ブラウザのバージョンアップや、安易に危険な Web サイトにアクセスしないということなどに気を付けないと甚大な被害に遭ってしまうと感じたので、気を付けていきたいと思います。
- 脆弱性など知識としてはあったものの、実際にサイバー攻撃を受けた際に何をすれば良いのか分からなかった。サイバーセキュリティの勉強を始めたこともあり今回の研修に興味を持ったのですが、研修に参加したことで当事者意識が生まれました。今後は実践としてのサイバーセキュリティ知識をもっと身に着けていきたいと思いました。

■まとめ

今回の研修ではサイバー攻撃によって Web サイトにアクセスした際に別のサイトに飛ばされましたが、その段階ですでに強制的にマルウェア（ウィルス）を自動でダウンロードされるようになっていました。サイバー攻撃を受けた際に「一番やってはいけないこと」は、ファイルを削除する・電源を切る・LAN ケーブルを抜いてしまうなどです。この行動をしてしまうことにより、原因が突き止められなくなります。

【報道関係者各位の問い合わせ先】
株式会社サイバーセキュリティクラウド　経営企画部　広報担当：竹谷・川﨑
TEL：03-6416-9996　Mobile：080-4583-2871(川﨑携帯)
FAX：03-6416-9997　E-Mail：pr@cscloud.co.jp

皆さんにお願いしたいのは、システムは古いバージョンのものを使用していると、そこが脆弱性となるため新しいバージョンにアップデートしてもらえたらと思います。それこそ皆さんが簡単に始めることの出来る「サイバー攻撃対策」の 1 つです。

また今回の研修の通り、サイバー攻撃は実際に「目的を達成する為の行動が表面化」してからは、あっという間に進んでしまいますが、そこに至るまでに長い期間をかけて準備がなされる傾向にあります。日頃よりサイバーセキュリティに関する意識を強く持ち、まずは「出来ること」からサイバー攻撃対策を進めていくことを強くお勧めいたします。

■株式会社サイバーセキュリティクラウドについて

住所　　：　東京都品川区上大崎 3-1-1 JR 東急目黒ビル 13 階
代表者　　：　代表取締役社長 兼 CEO 小池敏弘
設立　　：　2010 年 8 月
URL　　：　https://www.cscloud.co.jp/

サイバーセキュリティクラウドは「世界中の人々が安心安全に使えるサイバー空間を創造する」という経営理念を掲げ、世界有数のサイバー脅威インテリジェンスと AI 技術を活用した、Web アプリケーションのセキュリティサービス、及び脆弱性情報収集・管理ツールといったハッカー対策サービスを提供しています。これからも私たちは WAF を中心としたサイバーセキュリティにおけるグローバルリーディングカンパニーの 1 つとして、情報革命の推進に貢献してまいります。

主な展開サービス：
- クラウド型 WAF『攻撃遮断くん』：https://www.shadan-kun.com
- パブリッククラウド WAF の自動運用サービス『WafCharm』：https://www.wafcharm.com
- 改竄検知機能を搭載した『WafCharm for AWS Marketplace』：https://www.wafcharm.com/jp/aws-mp
- 厳選された AWS WAF 用のルールセット『Cyber Security Cloud Managed Rules for AWS WAF』：https://aws.amazon.com/marketplace/seller-profile?id=baeac351-6b7c-429d-bb20-7709f11783b2
- 脆弱性情報収集・管理サービス『SIDfm』：https://sid-fm.com

【報道関係者各位の問い合わせ先】
株式会社サイバーセキュリティクラウド　経営企画部　広報担当：竹谷・川﨑
TEL：03-6416-9996　Mobile：080-4583-2871(川﨑携帯)
FAX：03-6416-9997　E-Mail：pr@cscloud.co.jp