Security Days Tokyo Spring 2024

2024 年 3 月 15 日　於 JP タワーホール＆カンファレンス

1.サイバーセキュリティの最新動向と人材育成　情報通信研究機構 執行役 盛合 志帆 氏

【講演概要】

国の機関である情報通信機構（NICT）でもサイバーセキュリティ対策を研究し、民間に提供している。日本ではまだ、経営トップのセキュリティに対する意識とリーダーシップが弱い。ひとたび被害にあえば、企業の経済損失は莫大だ。つまり、**セキュリティはすなわち経営問題である。**被害額は 500 万円以上が過半数。攻撃者の分業化が進み、ビジネスになっている。その証拠に、RaaS と言う犯罪のサービス基盤ができ上っている。

NICT の取り組み。①サイバー攻撃のリアルタイム監視。②ダークネットを監視。③サイバー攻撃の傾向把握。ダークネット IP アドレス数：289,686。14 秒に 1 回の攻撃を観測。

直ぐにできる IoT 機器セキュリティ対策 7 選。①IoT 機器の再起動。②ファームウェアのアップデート。③パスワードの変更。④インターネットからのアクセス拒否。⑤ゲートウェイの採用。⑥古い機器は交換。⑦注意喚起には即対応。⇐ **常識的な事ばかり。**

産学官の連携拠点形成に向けて日本に必要なことは以下の通り。

① 実データを大規模に収集・蓄積する仕組み
② 実データを定常的・組織的に分析する仕組み
③ 実データで国産製品を運用・検証する仕組み
④ 実データから脅威情報を生成・共有する仕組み
⑤ 実データによる人材育成をオープン化する仕組み

NICT でも人材育成のカリキュラムを設けてサイバーセキュリティ技術者の育成を進めている。

① 実践的サイバー防御演習。② 情報処理安全確保支援士向け特定講習。③ 演習教材提供。

最後に　**セキュリティ解析者を日本でも人気職業に！**　を目指している。

【ポイント】

国レベルでも結構な人とお金をかけてセキュリティ対策を進めている。こうした動きがあまり伝わってこないのはなぜか。情報は普通の人の PC、スマホから最初に漏洩する場合が多い。**メディアでもこうしたことの注意喚起をする必要がある。**

2. フィッシング攻撃から組織を守る仕組みづくり　Cofense inc マーカス ヴォート 氏

【講演概要】

【Cofense とは】Cofense は従業員のセキュリティ意識を活用し、メールフィルタリングをすり抜けた攻撃メールへ、プロアクティブに対処するためのサービス。

クレデンシャルフィッシング：クレデンシャル・フィッシング（phishing）は、攻撃者がデジタル操作と心理的な圧力を駆使してユーザーの防御を破り、攻撃の餌食になるように仕向けるフィッシング攻撃。最近では、**フィッシング攻撃の 96%が、信頼できる組織を装った不正なメール（クレデンシャルフィッシング）から始まっている。**

モーフィングアタック：顔認証システムなどを攻撃する手法で、顔画像を変形させ認証をすり抜ける技術。

これらの進化する攻撃を防御するには**集団で守ることが最も効果的だが、必ず集団の中でも引っかかる人は存在する。**これをどう防ぐか？　その解の一つが Cofense である。

メール訓練内製化・不審メール初動対応支援ソリューション Cofense / サービス・製品 / 情報セキュリティの NRI セキュア（nri-secure.co.jp）

【ポイント】

必ず騙される人は存在する前提で、社内のセキュリティ防御を考えないといけない。外部サービスの利用もその一つである。

3. クラウドセキュリティの最前線　Cloudbase COO　小川 竜馬 氏

【講演概要】

クラウドサービスの脆弱性、設定不備をついたセキュリティ攻撃が後を絶たない。

対策としては

- ストレージの公開範囲と認証設定の監視
- 最新の攻撃情報を元に、データベースの脆弱性診断
- ネットワークのアクセスを監視し、不正な行動の事前検知

しかし、こうした対策は人員がいない、費用が取れないなどの理由でなかなか自前では実行できない。こうしたクラウドの管理は外部の専門家に任せるのが、最も費用対効果が高い。

【ポイント】

確かに現実的には、専任部署でもない限り、自前でこうした運用を行うのは難しい。こうしたサービス会社が登場してくるのも、それだけ要望があるということなのだろう。

4.いま世界で起きているサイバー犯罪とシマンテックのゼロトラスト （パネルディスカッション）

・SB テクノロジー 辻 伸弘 氏・SB C&C 山名 広朗 氏・シマンテック ロブ グリー 氏
・マクニカ 星野 喬 氏

【講演概要】

最近のセキュリティトレンドでは生成 AI を意識したセキュリティ対策が目立って来ている。対処としては　・セキュリティガードレールの設定。　・データバンクの再チェックなどが必要になる。しかし AI を使われると、更に対応が難しくなる。

・SASE： SECURE ACCESS SERVICE EDGE（SASE サッシー）：システム環境がデータセンターからクラウド中心に変化しているため（＝アクセスフリー）、セキュリティ環境も柔軟な対応を迫られる。そのため SASE のような、エッジでの対策が必要になる。つまり SASE の機能は、ユーザーのトラフィックは近くのポイントでセキュリティが検査され、そこから宛先に送信される。これは、アプリケーションとデータへのアクセスがより効率的になることを意味し、分散した従業員とクラウド内のデータを保護するためのより優れた対策となる。更に必要な対処は

・ID 管理をクラウドシフトすることである。具体的な方法は以下のようなものになる。

・1. シングルサインオンで管理コストを減らす

・2. クラウドサービス側でアクセス制御を行う

https://www.idearu.info/article/system/cloud-id-password

ラテラルムーブメント攻撃は、初期の不正アクセスを得た後、サイバー犯罪者がアクセスの持続性を維持し、組織のネットワーク内を横断的に移動するための多段階のプロセスで構成されている。ラテラルムーブメントの一般的なステップは以下の通り。

ラテラルムーブメントとは？具体的な手口や危険性、対策について徹底解説｜サイバーセキュリティ.com (cybersecurity-jp.com)

① 初期の侵害

ラテラルムーブメント攻撃の最初の段階は初期のネット内への入り込み。サイバー犯罪者は、フィッシングメール、ソーシャルエンジニアリング、イニシャルアクセスブローカー（IAB）、またはソフトウェアアプリケーションの脆弱性を利用して、従業員のデバイスやアカウントを攻撃し、不正なアクセスを得て、ネットワーク内に侵入し、偵察やさらなる攻撃を目的とした他のツールを使用したり、ネット内での足場を築く。

② 偵察

偵察の段階では、攻撃者は目標とした環境に関する情報を収集する。これには、対象に関する公共の情報の収集、ネットワークのスキャンによるマッピング、オープンポートの検索、およびそれらの上で実行されている脆弱なデバイスやサービスの識別が含まれる。

③ クレデンシャルハーベスティング

ネットワークインフラ内でのラテラルムーブメントを容易にするために、適切な権限を持つ有効なユーザー認証情報（ユーザー名/パスワード）をさまざまな手段を使用して、組織のパスワードポリシーの弱さを悪用して取得する。

④ パスワードスプレー攻撃

攻撃者は一般的に使用されるパスワードを多くのアカウントに対して同時に複数回のログイン試行で使用し、アカウントのロックアウトが発生せずに機能するものを見つけるまで続ける。

⑤ 脆弱性の悪用

攻撃者は有効な認証情報を取得したら、しばしば権限を昇格させる。攻撃者はネットワーク内の他のデバイスで機密データにアクセスしたり、コマンドを実行したりして、効果的に影響を横断的に複数のシステムに広げる。

⑥ 持続性とデータ漏洩

ラテラルムーブメント攻撃の最終段階は、侵入したシステムから貴重なデータを持ち出すため、将来のアクセスのためのバックドアを作成し、接続の持続性を確立することを図る。リモートアクセス用のランサムウェアや RAT（遠隔操作ウイルス）のような悪意のあるソフトウェアを導入して、侵入したマシンを遠隔で制御し、組織の IT ネットワークに持続的な足場を築くこともある。

【ポイント】

攻撃者は単純にマルウェアを入れ込み、システム障害をおこすだけでなく、長期にわたって、システムに居続け、気づかれずにシステムを操り続けることを企んでいる。**こちらもその覚悟でセキュリティ対策をとらないと対応できない。**

5.AI 技術と次世代型 SIEM で描くセキュリティ戦略　　クレスコ 宮本 雄仁 氏

【講演概要】

マルウェア対応は以下の手順で行う。

攻撃対象の特定⇒防御手段選択⇒検知手段⇒対応手段⇒復旧手段　この全体がセキュリティガバナンスになるが、これを人手でやるのは大変。Sumo Logic ではこれを AI を使って効率化する。適切な対応手順を ChatGPT が文章化して示す。

【以下 Sumo Logic の HP の説明文】フルスタック Cloud SIEM（Security Information and Event Management シーム）

【Sumo Logic は、あなたにとっての最初のクラウド SIEM として最適です。さらに従来の SIEM との置き換えや、既存の SIEM ソリューションとの共存も可能です。】

・AWS、Azure、GCP、SaaS など向けのクラウドセキュリティの監視

・統合された脅威インテリジェンス

・PCI コンプライアンス

・インシデント対応と自動化ワークフロー

などを行うことが可能です。

セキュリティインテリジェンス ｜Sumo Logic

【ポイント】

主だったクラウドサービスの運用状況を可視化するクラウドサービスは高度化するクラウドの運用をスムースにするには必要なサービスかもしれない。

6. 特権アクセス最前線　　エンカレッジ テクノロジ　佐藤健太郎 氏

【講演概要】

顕在化してきたクラウド利用時の課題は以下の通り。

設定ミスによる情報漏洩

クラウドの設定が不適切なため、本来機密性を担保しなければならない情報が誰でも閲覧できてしまう状態となってしまう。

過剰な権限付与

本来、必要最小限の権限のみを付与すべきところに、過剰な権限を与えてしまったため、不正アクセスによって付与された権限を使用されてしまう。

安易な認証情報

さまざまなサービスで同じパスワードを設定いる。

複雑性が不足しており、推測されやすいパスワードを使っている。

認証キーの不適切な取り扱いをしている。

【ポイント】

こうした細かい対応も含め、専任の部門がない中小の会社ではクラウド管理の対応が難しい。中小と言えども、大企業のサプライチェーンの一部を担っている可能性もあり、セキュリティ問題に適切に対処する責任が発生する。

7. サイバーセキュリティ対策と組織マネジメント　　フリー 茂岩　祐樹 氏

【講演概要

ランサムウェア対策は総力戦。一度感染してしまうと、

① 機会損失、契約不履行問題が起きかねない。

② 機密保護違反で訴訟になるかもしれない。

③ 個人情報保護違反で刑事事件になりかねない。

④ 評判を落とし経営の足かせになる。

⑤ 財務基盤を毀損する。

などの問題が考えられ、単に情報部門だけ問題ではない。**全社の問題であり、全社で取り組むべき問題である。**

【ポイント】

まさにその通り。全社員に関係する問題であり、感染のリスク対策は全員で取り組まねばならない。しかも、一般の従業員の PC などから感染する割合が高いことから、IT 部門だけが取り組めばよい問題ではなく、一般社員に対する日ごろからの意識づけ、訓練が基本になる。

以上