［第 359 回朝食会結果］

サイバー犯罪の現状と企業のセキュリティ対策を研鑽しました!

神奈川県警サイバーセキュリティ対策本部大和弘路警視をゲストに開催

ようやく秋らしい気候となった１０月１７日(火)８時１５分より、HOTEL THE KNOT YOKOHAMA において 46 名の出席で開催いたしました。

加藤会長の挨拶、初参加の挨拶、事務局報告を行い講演に入りました。今回のテーマは、インターネットや高度情報通信ネットワークが企業の業務合理化も含め利便性を急速に向上させ、社会・経済の根幹を支えるインフラとして機能している一方で、フィッシング詐欺等のサイバー犯罪（高度情報通信ネットワークを利用した犯罪やコンピュータ又は電磁的記録を対象とした犯罪等の情報技術を利用した犯罪）が、年々その深刻さを増し犯罪の検挙数は増加の一途をたどっていることから、神奈川県警察サイバーセキュリティ対策本部 企画担当管理官 大和 弘路警視(写真上)をゲストに「サイバー犯罪の現状と企業におけるセキュリティ対策」と題して開催いたしました。(以下、講演の要旨です)

盗み取られた資金がミサイルの実験や紛争の資金になっているかもしれない！？

神奈川県警の大和です、「サイバー犯罪の現状と対策」について、お話をさせていただきます。

最初に、サイバー空間の脅威、現状ですが、神奈川県警の令和４年中のサイバー事案の相談は 8,886 件で非常に増加しております。原因として、テレワークなどの仕事の在り方の変化、ネットショッピングや電子決済などによって、実生活や社会経済活動が変化してきたことが考えられます。

あまり話題には上がってきませんが、一部では、国家を背景としたハッカー集団が窃取した暗号資産がミサイルの発射実験や紛争のための資金になっているのではないかという報道があります。サイバー犯罪の被害に遭わないように、個人や企業の資産を守る、ということが大前提ですが、盗み取られた資産がミサイルの実験や紛争の資金に回ってしまうかもしれないという考え方も頭の片隅に置いていただきたいと思います。

今年の７月には、サイバー攻撃によって、名古屋港の貿易拠点の物流がストップしました。サイバー攻撃によって、社会経済活動にも大きな影響を与えてしまいます。

こうした話をすると、犯罪集団は捕まるのか？という質問を受けることがあります。情報を抜き取った上、ファイルを暗号化して、それを復号することと引き換えに身代金を要求する「ランサムウェア」に関しては、令和３年以降、欧米などの捜査機関が合同捜査を行い、いくつかの犯罪グループを検挙しています。それでも、１つのグループのメンバーを検挙するのに数年はかかっているのが現状です。サーバを押収したものの、グループのメンバーの検挙に至っていないものもあります。また、「エモテット」（主にメールの添付ファイルを感染経路とした不正プログラム）に関しては、令和３年２月に、サーバコンピュータを止めるテイクダウンということが行われ、メンバーが拘束されたとも報道されています。

では日本はどうなのかというと、令和４年４月に、警察庁にサイバー局を発足させ、いわゆる日本警察としてのサイバー捜査部門である「サイバー特別捜査隊」を創設して、国際的な協力関係を構築して捜査を行っています。

報道もされていますが、サイバー特別捜査隊では、北朝鮮ハッカー集団「ラザルス」の関与を捜査して、攻撃の抑止や手口の周知、その対策につなげるため、「パブリック・アトリビューション」という非難声明を行いました。この他、捜査情報を国際的な捜査機関に提供して被疑者を訴追したり、共同声明を出すなど成果を上げているところです。今回、ここで紹介した内容は、ネットニュースでもアップされているので、興味があったら見てください。

※講演以降に、国際共同捜査で、ランサムウェアのウイルス開発者の逮捕についても報道されていますので、興味があればこちらも見てください。

ランサムウェア被害では、システムの復旧に１週間以上の期間を要した企業等が約８割！そして、システムの復旧に 1,000 万円以上の費用を要した企業等が約５割！！

これまでに、セミナーなどを通じて、経営者様と意見交換をしてきたところ、「ウチはサイバー攻撃を受けるような大企業ではないし、盗まれて困るような重要な情報もない。」や「システムは外部委託なので大丈夫。」「大手に依頼しているから大丈夫。」や「ウイルス対策ソフトを入れているから大丈夫。」という意見を聞く機会がありました。

どうしてもサイバー攻撃と聞くと、高度なハッカー集団によるイメージが強いので、こうした意見が多くなるのだと思いますが、ランサムウェアやフィッシングのマニュアルを手にして、サイバー犯罪をビジネスとする犯罪組織が増えてきています。特殊詐欺をイメージすれば分かりやすいのですが、特殊詐欺もマニュアルの存在がたびたび報道されていると思います。

犯罪組織から見れば、確実にお金が取れればいいのです。大企業であろうが、小規模事業者であろうが、お金さえ取れればいいので、セキュリティの甘いところを探して、そこを狙うのです。

皆様方の企業がセキュリティに取り組まれていても、サプライチェーンの関連企業や取引先の企業の中で、セキュリティ意識の低いところがあれば、そうした企業を通して皆様の企業が狙われることも十分にあります。だから、皆様を取り巻く企業の方々にも、セキュリティ対策の意識を広めていただきたいというのが実情です。

ランサムウェアの被害報告件数ですが、警察庁の統計では、令和４年中は全国で 230 件となっています。これはあくまでも警察に届け出た件数なので、被害が潜在化している可能性があります。１分１秒でも早く復旧させて業務を再開したいので、復旧作業の請負業者には連絡が行きますが、実際の被害状況は分からないのです。県内のある市町村が、サイバー攻撃の被害に関するアンケートをとりましたら、回答のあったうちの、約２割の企業が被害に遭ったとの回答が出ています。これは報道もされていますが、こうした現状を考えると、神奈川県内では、おそらくかなりの数の被害が遭ったのではないかと推察できます。

警察庁が公表した資料では、被害に遭ったときにシステムの復旧に要した期間は、即時～１週間が２６％、１週間～１か月かかったものが２５％、１か月～２か月かかったものが１６％、２か月以上かかったものが１１％となっていて、被害に遭ったときの影響は非常に大きいというのが実情です。

また、システムの復旧に要した費用は、100 万円未満が２４％、100 万円以上 500 万円未満

が１６％、500 万円以上 1,000 万円未満が１４％、1,000 万円以上 5,000 万円未満が３３％、5,000 万円以上が１３％となっており、やはり被害に遭ったときの影響は非常に大きいというのが実情です。

VPN機器が設置されていますか？確認してください！バージョンが古いと狙われます！！

まずは、自社にＶＰＮ機器が設置されているかどうか確認をしてください。システムの担当者の方が分かると思いますが、ただ、中には、とりあえずシステム担当者という役割を任せている場合もありますので、とりあえずＶＰＮ機器が設置されているか確認をお願いします。もし、設置されていれば、ＶＰＮ機器のバージョンがいくつなのか確認をしてください。分からなければ、外部の委託会社など設置した会社に確認をしてください。バージョンが更新されていなければ、パッチを当てる、という言い方をしますが、バージョンの更新を行ってください。

なぜ、こうした確認のお願いをしているのかと言うと、ランサムウェア被害の被害実態を確認すると、被害に遭っている企業等の約６割が、ＶＰＮ機器からシステムに侵入されています。ＶＰＮは、分かりやすく言うと、通信を盗み見されないようにする通信技術です。その通信技術を使う機器がＶＰＮ機器です。テレワーク、リモートワークを導入しているとＶＰＮ機器が設置されている場合が多いと思います。また、取引先からの依頼でＶＰＮ機器を設置していたり、遠隔保守用に外部委託会社がＶＰＮ機器を設置している場合があります。

保守契約を確認することも大切です。保守契約がなければ、委託会社もバージョンの更新を行いません。我々の調査では、委託会社と保守契約があったにも関わらず、バージョンの更新を失念していたケースもありました。ＶＰＮ機器が設置されているのであれば、必ずバージョンの更新状況を確認してください。

玄関のドアをイメージしてください。昔、ピッキングというものが流行り、玄関のカギもピッキング対策が施されているカギが増えてきたと思います。また、サムターン回し防止や２か所カギをかけるようになったり、犯人も玄関から侵入するために玄関ドアの色々な弱点を探すのですが、玄関のドアも被疑者に突破されないためにバージョンアップしていると考えれば分かりやすいと思います。車のキーも盗難防止のために色々とバージョンアップしています。これと同じです。

コロナ禍から業務形態が変わってきて、ＶＰＮ機器を設置する企業が増えてきたのですが、犯罪組織は、ＶＰＮ機器から侵入するために弱点を常に探していますので、必ず設置の有無とバージョンの確認をするようにお願いします。

ただし、バージョンの更新をお願いしているのですが、バーションを更新することによって、他のシステムやソフトが動かなくなる場合があります。バージョンを更新する際には、必ずシステムの管理会社などと相談をして影響がないことを確認してから行ってください。

また、ぜひ、お取引先にも、ＶＰＮ機器のことについて、お声をかけてください。よろしくお願いいたします。

アクセス制限を設定していますか？確認してください！管理者の権限を乗っ取られたら、お城の本丸を落とされたも同じです！！

実は、今や社内システムに侵入されることを１００％防止することできないと考えられています。また、自宅を事例に出しますが、空き巣に入られた時のために、貴重品を分かりやすいところに置かないという防犯対策があります。これは、空き巣に入られることが前提となっていますが、これ

と同じで、社内システムも侵入されたときのことを考えなければいけません。
　システムに侵入されて一番怖いのは、「システムを統括する権限」が乗っ取られることです。ここでは、「管理者の権限」とお伝えします。とにかく、この権限を守ることが大切です。簡単に言うと、犯罪組織がシステムに入り込んで、この管理者の権限を自由に使うことが出来てしまえば、社内のシステム全てを、自由に使えるようになってしまいます。そうすると情報を盗んだり、データを書き換えたり、暗号化されたりしてしまうという感じです。
　これまで被害に遭った企業の中には、この管理者の権限に、従業員が簡単にアクセスできる状態になっていた例がありました。
　極端な例えにすると、社長と経理担当者と営業担当者がいたとします。問題になるのは、経理担当者も営業担当者も、仕事で使っているパソコンで、社長が行っている仕事の中身が見れてしまうという状態です。これだと、営業担当者がメールのやり取りなどをきっかけにして、犯罪組織に侵入を許した場合に、簡単に社長が持っている大事な情報などを盗み取られてしまいます。もし、これが、営業担当者は、営業担当者の業務で使うファイルやシステムにしかアクセスできない、経理担当者も業務で使うファイルやシステムにしかアクセスできない、というようにアクセスに制限を設けていれば、社長が使うファイルやシステムにはアクセスできません。そうすると、営業担当者がメールのやり取りなどをきっかけにして、犯罪組織に侵入を許したとしても、社長が使うファイルやシステムにはアクセスすることができなくなります。
　ぜひ、社内で誰がどの情報にアクセスできるのか確認をして、部署や役職などによって、アクセスの制限を行って、管理者の権限を乗っ取られないように、しっかりと守るようにしてください。

みんなで共通のパスワードを使っていないですか？簡単に予測できるようなパスワードを使っていないですか？

　さきほど説明したアクセス制限に話の趣旨が似ているのですが、こちらは、パソコンにログインするとき、メールソフト立ち上げるときなど、ＩＤとパスワードを入力して社内のネットワークなどを利用していると思います。
　問題になるのは、従業員みんなが同じパスワードを使用している場合です。例をあげると、何らかの作業をシステムの管理会社などに依頼すると、納品を受けたときに、ＩＤとパスワードを記載したファイルをデスクトップに置いていることがあり、それを、そのまま従業員で使っていることがあります。この場合、いくらアクセス制限を設けていたとしても、そのＩＤとパスワードを使えば管理者の権限を使うことが出来てしまいます。
　また、パスワードを個別に設定していたとしても、キーボード配列で、１２３４５６７８９０とか、その逆で０９８７６５４３２１などは簡単に予測されてしまいます。また「１ｑａｚ２ｗｓｘ３ｅｄｃ」などは一見複雑に見えますが、これもキーボードの「１のキーから順に下にＱＡＺと押して、次に２のキーから順に下にＷＳＸ、次に３のキーから順に下にＥＤＣ」と入力したものです。パソコンのキーボードを見てもらえれば分かると思います。このほか、「ｐａｓｓｗｏｒｄ」、「ｐ@ｓｓｗｏｒｄ」、「ｐａｓｓｗ０ｒｄ」のようにパスワードという英単語に少し手を加えたものなども簡単に予測されるパスワードです。
　犯罪組織は、こうしたみんなが考えそうなパスワードを大量にリスト化していて、システムに侵入したら、これを大量に入力してくる手口も使います。だから、しっかり個別にＩＤとパスワード

を設定する、予測できるようなパスワードは再設定する、と社内教養を行っていただきたいです。
　また、国が奨励しているのは 10 桁以上としていますが、急激に発達している情報通信技術を考えれば、解析速度はさらに加速すると思うので、やはり１０桁以上のパスワードを作ってくださいとお願いしています。

アカウントロックの機能を設定すれば、パスワードを破る攻撃を防ぐことができる！？

　スマートフォンなどを使っていて、ＩＤとパスワードの入力を３回間違えたらロックが掛かってしまったということを経験したことがあると思います。まさにこの設定です。
　さきほど、犯罪組織がパスワードを破るのに、みんなが考えそうなパスワードを大量にリスト化して、次々に入力する攻撃などを仕掛けてくると説明したのですが、こうした攻撃を防御するために、３回ＩＤとパスワードの入力を間違えたらアカウントロックするという設定をしてください。
　「ウチにＶＰＮはあるのか、ないのか。バージョンはどうなんだ。」、「アクセス制限はどうなっているのか」、「ＩＤ・パスワードは分かりにくいもので設定しているか」、「アカウントロックの設定はどうなのか」など、経営者側の皆様が関心をもってシステム担当者などに確認をすることによって、セキュリティに対する意識は上がると思います。

「セキュリティアクション」に取り組むとIT（セキュリティ）関連の補助金を申請できるメリットが！！

　現在、県内の中小企業・小規模事業者の約４割が会員となっている県内の商工会議所・商工会を回っています。サイバーセキュリティに関する実態把握とニーズ調査を行っています。また、各種セミナーでは、機会によって、参加した経営者様からもサイバーセキュリティに関する情報交換を行いました。生の意見として、経営者様からは、サイバー関係の危険性は認識しているし、取り組まなければならないことは分かっているが、横文字が多くてとっつきにくい、そもそも何をやっていいか分からない、セキュリティ関係はお金がかかる、メリットがない、という意見がありました。特にメリットがないという意見は多く、警察としては、被害に遭わないことが、損失を出さないという観点からもメリットになるのではないかと思っていましたが、純粋にセキュリティに取り組んでも利益があがらないという考え方は、逆に新鮮でした。
　お金がかかるとか何をやっていいのか分からないという意見については、これまでにお話をさせていただいたことをお伝えしてきました。そして、メリットを感じていただくためには、なんだろうと考えましたが、セキュリティに関する機器などの導入補助金の交付があることは、メリットになるのではないかと思い、お伝えするようにしてきました。
　そこで、提案しているのが、IPA(独立行政法人情報処理推進機構)が推進している「セキュリティアクション」に取り組むことをお願いしているところです。
　まず、取り組むことによってＩＴ導入の補助金の申請の要件になります。それと、取引先から契約条項でセキュリティへの取組も求められることが増えていますが、取り組んでいる姿勢の評価を受けることもあると聞いています。企業価値を高めるという意味ではメリットもあると思います。
　ネットで「ＩＰＡ」を検索すると、ＩＰＡのホームページでセキュリティアクションの取組方法が掲載されています。取り組みますと一つ星★、二つ星★のマークを名刺やパンフレット、ホームページに掲載することができるので、取組を周知することができます。

[一つ星]は、「情報セキュリティ５か条」に取り組むことを宣言します。宣言することをＩＰＡに報告すると１つ星を獲得することになります。
① OS やソフトウエアを常に最新の状態にすること、② ウイルス対策ソフトを導入すること、③ パスワードを強化すること、④共有設定を見直すこと、⑤脅威や攻撃の手口を知ること、です。①はＶＰＮの部分、あと③と④は今回お伝えしたとおりです。⑤は後で趣旨をお伝えします。

[二つ星]は、25 個に診断項目が増えるのですが、診断項目に沿って自社のセキュリティの問題点を確認していきます。次が、少しハードルが上がるのですが、「情報セキュリティポリシー」を定めて企業や組織において実施する情報セキュリティ対策の方針や行動指針をＩＰＡに送ります。

ちょっと、「うっ」となるのですが、実は、ＩＰＡにちゃんとひな形があるので、それに当てはめていけば意外とできます。サポートもしてくれますので、まず、セキュリティアクションに取り組んでいただくことがセキュリティの意識を高める第一歩だと思います。

サイバー攻撃の手口を知ることが大切！何に取り組んでいこうか見えてきます！！

セキュリティアクション１つ星の⑤にもありますが、相手の攻撃の手口を知ることも大切です。技術的な理解は後回しで結構です。私も技術者ではありません。気をつけるべきことが何となく分かってきます。サイバー攻撃にはどんなものがあるのか、パスワードを攻略するブルートフォース（総当たり）攻撃、パスワードスプレー攻撃、辞書攻撃や、メールを悪用して攻撃する標的型攻撃、高度標的型(ATP)攻撃、そして、ホームページやウェブサイトを悪用して攻撃するＳＱＬインジェクション、水飲み場攻撃、ＭＩＴＢ攻撃など、本当にたくさんあります。

野球やサッカーなどのスポーツや格闘技、将棋なども、相手の攻め方を知っていれば、その対策を考えることもできて、興味のある分野であれば、さらに知識が増します。ネット検索で色々見てみると、興味が湧いてくると思います。

被害に遭ったら復旧作業の請負業者への連絡だけでなく、会社の所在地を管轄する警察署の生活安全課に必ず相談・連絡を！！

これは皆様にお願いですが、冒頭でお伝えした通り、警察には殆ど被害状況は入ってきません。皆様にとっては１分１秒でも早く復旧させて業務を再開したいので、復旧作業の請負業者には連絡が行きますが、警察にはなかなか連絡がありません。また、警察に連絡して捜査が入ることで被害に遭ったことが公に出てしまい取引先からの信用を失ってしまうのではないか、という意見も聞いています。とは言いつつも、復旧作業の請負業者への連絡だけでなく、管轄警察署の生活安全課に必ず相談・連絡をしていただきたいのです。

冒頭で示したように、即時復旧はほぼ見込めないという統計があるので警察に連絡するデメリットはないと思っています。我々が臨場しても業者の邪魔をすることはしません。並行して証拠保全するようにしています。連絡をいただければ、捜査情報をサイバー特別捜査隊に集約して、海外の捜査機関と協力することができます。日本だけが泣き寝入りするようなことがあってはいけないので、ぜひ警察にも連絡・相談をお願いいたします。

また、社内での研修や業種ごとの集まりなどがあれば、お話をさせていただきますので、そうした機会があれば、ぜひ、神奈川県警察サイバーセキュリティ対策本部(045-211-1212 内線６３２７)に御連絡ください。