ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●衣料品ストアの社内ネットワークに不正アクセス、ランサムウェアか… キャッシュレス決済停止等影響

https://www3.nhk.or.jp/news/html/20220510/k10013620031000.html
https://www.shimamura.gr.jp/assets-c/uploads/74c0907543e766d3f9d0fd5df3e5faac964b4a0c.pdf

このニュースをザックリ言うと･･･

- 5月11日(日本時間)、大手衣料品ストアチェーンのしまむらより、同4日に社内ネットワークが不正アクセスを受け、システム障害が発生していると発表されました。
- 障害状況確認のため、同社グループ店の「しまむら」「アイベル」等では同5日にキャッシュレス決済の一時停止を行い、6日には安全が確認され再開されていますが、商品取り寄せについて引き続き影響が出ているとのことです。
- なお、社員・利用客・取引先に関する情報・個人情報の流出は、この時点では確認されていないとのことです。
- 前日のNHKの報道等によれば、サイバー犯罪グループ「LockBit2.0」が同社から情報を盗み取ったことを宣言したとされており、同グループのランサムウェア攻撃を受けた可能性が指摘されています。

AUS便りからの所感等

- 同社では「経営及び店舗の営業に与える影響が少なく、また、犯罪者集団の増長を招くことを考慮し、当社からの情報開示は最低限にとどめております」としており、障害・被害の規模についての詳細は不明です。
- 昨年10月には地方の病院で電子カルテシステムがランサムウェアに感染(AUS便り 2021/11/09号参照)した結果、システムの復旧に2ヶ月かかる事態となっています。
- JPCERT/CCでは今年1月に「侵入型ランサムウェア攻撃を受けたら読むFAQ」が発表されていますが(同2022/01/25号参照)、依然としてランサムウェア攻撃と被害が度々報じられる現状、各組織においては攻撃を受ける前にFAQの読み込みを行うとともに、データのバックアップとその確実な保全、および確実に復旧できる体制等を整えることが肝要です。

NHK

衣料品「しまむら」ランサムウエアによるサイバー攻撃受けたか

2022年5月10日 19時10分

大手衣料品チェーンの「しまむら」は、大型連休中に社内のシステムの一部に障害が発生し、その影響で、店舗でのキャッシュレス決済などができなくなったことを明らかにしました。ランサムウエア、身代金要求型のコンピューターウイルスによるサイバー攻撃を受けたと見られます。

さいたま市に本社を置く大手衣料品チェーン「しまむら」によりますと、大型連休中の今月4日の夜、サイバー攻撃を受け、社内のシステムの一部に障害が出たということです。

被害の状況を確認するため、すべてのシステムを止めたことから、5日に全国におよそ2200ある、すべての店でキャッシュレス決済や商品の取り寄せの手続きができなくなったということです。

●2021年のフィッシング攻撃、前年より29%増加、小売・卸売業界への攻撃激増…Zscaler社発表

https://prtimes.jp/main/html/rd/p/000000031.000055108.html

このニュースをザックリ言うと・・・

- 5月12日(日本時間)、クラウドセキュリティベンダーの米Zscaler社より、同社の調査チームThreatLabzによる「2022 Zscaler ThreatLabz フィッシングの現状レポート」が発表されました。

- 2021年のフィッシング攻撃は2020年に比べ29%の増加となり、ターゲット組織の業界別で最も多かった小売・卸売業界に限れば増加率は436%にも上りました(この他金融系と政府機関が約100%の増加となった一方、ヘルスケア部門は59%の減少となっています)。

- また国別では上位から米国・シンガポール・ドイツ・オランダ・イギリスが最も多くターゲットとされた一方、オランダはフィッシング攻撃が前年比で38%減少したとしており、同国においてインターネット詐欺の罰則を強化する法律が可決されたことが要因と推測しています。

AUS便りからの所感

- 同レポートでは、自前で攻撃基盤を構築しないフィッシング攻撃を行う攻撃者に対し、ダークウェブ等で出来合いのツール・サービスを販売する「Phishing as a Service」の台頭についても取り上げています。

- 日本国内においても、4月に報告されたフィッシングの件数がついに9万件台に上ったとするフィッシング対策協議会の報告があり(AUS便り 2022/05/10号参照)、フィッシングを仕掛けられるユーザー側に対してはこれまで推奨されてきた各種防衛策(不審なメール・SMS等の受信時にはネット上での報告がないか確認する、利用するサービスはブックマークに登録してアクセスする)を改めて意識するとともに、ユーザーが所属する各社組織においてもメールサーバー等での防御ないし適宜ソリューションの導入によるユーザーの保護を確実に実施していくことが重要です。

フィッシング攻撃に関する2022年版レポートを発表：小売・卸売業界へのフィッシング攻撃が400%以上増加

世界規模でPhishing-as-a-Serviceを利用した攻撃が、重要な業界やユーザに対する主要な攻撃手口となっていることが判明

ゼットスケーラー株式会社

2022年5月12日 11時00分

- フィッシング攻撃が前年比29%増加し、昨年Zscalerクラウドで観測された攻撃は8億7,390万件という驚異的な数字
- 最も標的とされた小売・卸売業界では、過去12か月でフィッシング攻撃が400%以上増加
- フィッシング詐欺で最も標的にされた国は米国で、その次に高頻度で狙われたのは、シンガポール、ドイツ、オランダ、イギリス
- エンドユーザが不審なメールに警戒感を示すようになっている中、SMSフィッシングなど、新たなフィッシングの攻撃ベクトルが他の手法よりも速く増大
- 増大するフィッシング行為は、犯罪者にとっての技術的参入障壁を下げる、構築済みの攻撃ツールの市場が形成されているPhishing-as-a-Serviceの手法と直接関連

クラウドセキュリティ業界を牽引するZscaler（本社：米国カリフォルニア州、以下 ゼットスケーラー、https://www.zscaler.jp/）は本日、ゼットスケーラーの調査チームである「ThreatLabZ（読み方：スレットラボ・ゼッ

●「改正電子帳簿保存法」1月施行、請求書データ等の印刷保管禁止に

https://www.nta.go.jp/law/joho-zeikaishaku/sonota/jirei/pdf/0021012-095_03.pdf
https://w.wiki/5B2E (電子帳簿保存法・出典: フリー百科事典『ウィキペディア（Wikipedia）』)

このニュースをザックリ言うと・・・

- 国税関係帳簿書類を書面から電磁的記録(データ)での保存に代えるための規定を定めた、いわゆる「電子帳簿保存法(以下・同法)」が、1月1日(日本時間)より改正・施行されています。

- 領収書・請求書等の授受が電子メールでの受信やWebからのPDFダウンロード等で行われる、いわゆる「電子取引」のデータに関して、同法では受け取ったデータの保管を義務付ける一方で、これまで書面等に出力しての保管を代替手段として認める形がとられていましたが、今回の改正によりこの代替手段の規定が廃止されています。

- 改正に際し、2023年末までは「宥恕措置」が設けられ、それまでは電子取引データの印刷保管が認められるものの、税務調査等の際には要求されたデータを確実に提出できるようにする等、特定の条件を満たす必要があります。

AUS便りからの所感

- 今回の同法の改正は、電子帳簿保存開始3ヶ月前までに申請・承認を要する条項の廃止や、紙からのスキャンによる保存に関する様々な要件の緩和も大きなポイントとなっており、帳簿の電子化を促進するとともに、元々電子データであったものは電子データとして保管すべきという前提を改めて示したものとみられます。

- また、対象となるデータの保管にあたっては真実性と可視性の確保が求められ、後者の一例として、当該データを検索できる状態で保存すること、例えば受取日時や取引先企業名等が分かるようフォルダーの分類を行う等が求められる場合がある模様です。

- 法改正を機に、社内ネットワーク上やクラウド上に保存した各種データの流出・消去・改ざんを狙う攻撃がより顕著なものとなることが予想され、それに対する防衛もさらに重要となってきますので、もしも「全てのデータはローカルで保存しなければならない(そうすれば流出しない)」あるいは「データでの保存は不正アクセスで流出しやすいのに比べれば、物理で保存した場合の盗難等の方が難しいからリスクは低い」といったなんとなくの感覚・固定観念に囚われて情報を取り扱っていたのであれば確実に見直し、アンチウイルスやUTMを含めた多重防御で臨む態勢を整えることを今からでも計画すべきでしょう。