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。

●LAC元社員が社内ビジネス文書流出を持ち出し…フリーマーケット出品のHDDから発見

https://www.itmedia.co.jp/news/articles/2201/14/news151.html
https://japan.zdnet.com/article/35182127/
https://www.lac.co.jp/news/2022/01/14_press_01.html

このニュースをザックリ言うと･･･

- 1月14日(日本時間)、国内情報セキュリティ大手のラック社より、「当社より流出した過去の情報について」と題し、社内ビジネス文書が保存されたハードディスク(HDD)1台がフリーマーケットに出品されていた事案が発表されました。

- 同社の元社員が業務上のビジネス文書を社外に持ち出して個人所有のHDDに保存しており、当該HDDがフリーマーケットに売却されたのち、購入者からとみられる匿名の通報が2021年10月31日にあったと発表されています。

- 同12月17日に当該HDDは回収され、HDDから2003年～2017年に作成された内部ビジネス文書2,069件(うち取引先の文書628件)および個人情報最大1,000件(同社社員・取引先社員の社名・部署・氏名・メールアドレス・電話番号)が復元されましたが、該当する情報は元社員および購入者以外には渡っていないとのことです。

AUS便りからの所感等

- 国内情報セキュリティの老舗企業で発生した事案として少なからぬインパクトをもって取り上げられたニュースである一方、発覚からの迅速な対応により被害が最小限に食い止められたことは幸いであり、再発防止策として「業務データの複製の制限と監視の技術的対策の強化」「社員の異動や退職時等の機器の回収や情報廃棄など社内プロセスの強化」と積極的な内容を挙げていることはある意味面目躍如とも言えるでしょう。

- また一部ニュースによれば、元社員が社内と自宅とでオンラインストレージ「Dropbox」を利用していたことにより、自宅PCのHDDに社内文書データが同期されたとのことで、同社では社内からDropboxへのアクセスを禁止する対策をとったとしていますが、「個人で契約したサービスを企業内でも利用することによるデータの共有」を防ぐためには、そういったサービスへのアクセス禁止とは別に、会社で正式に有償サービス等を契約することにより、適切な管理と安全な利用が期待されるアプローチをとることも考慮に値します。

- この他にも「HDD(およびSSD)からの情報復元の可能性」にフォーカスするならば、企業や個人に拘わらず、またモバイル・ノートPCからデスクトップ・サーバーまで、機器の意図しない盗難・紛失をも考慮し、OSの機能等によるストレージの暗号化を可能な限り実施することは有用でしょう。

ITmedia NEWS

業務情報、フリマで流出　退職者がHDD売却　情報セキュリティのラックが謝罪

2022年01月14日 19時24分 公開　[ITmedia]

情報セキュリティ企業のラックは1月14日、同社の社内ビジネス文書が保存されたHDDがフリーマーケットに出品され、購入者に情報が流出したと発表した。HDDは回収済みで、情報の拡散はないという。

ラックは2021年10月31日、匿名の個人から「フリーマーケットで購入したHDDにラックのビジネス文書が入っていた」とする通報を受けた。通報者とのやりとりの中で情報流出があったと判断し、12月17日にはHDDを回収。通報者以外への情報の流出がないことを確認した。

HDDに含まれていた情報は、03年から17年に作成されたビジネス文書が2069件、同社社員や取引先社員の会社名、部署名、氏名、連絡先などの情報が最大1000件。

●「侵入型ランサムウェア攻撃を受けたら読むFAQ」JPCERT/CC公開

https://internet.watch.impress.co.jp/docs/news/1380952.html
https://www.jpcert.or.jp/magazine/security/ransom-faq.html

このニュースをザックリ言うと・・・

- 1月13日(日本時間)、JPCERT/CCより、「侵入型ランサムウェア攻撃を受けたら読むFAQ」と題した文書が発表されました。

- ランサムウェアによる攻撃の中でも「侵入型ランサムウェア攻撃」、即ち攻撃者が企業・組織の内部ネットワークに侵入して情報窃取やランサムウェアを用いたファイルの暗号化などを行うものについて、被害発生・発覚時の初動対策に特化したもので、「1. 被害を受けたら」「2. 被害への対応」「3. 関連情報」の3つのカテゴリー、さらに計9つのサブカテゴリーおよび17の項目からなっています。

AUS便りからの所感

- タイトルには「攻撃を受けたら」とは書かれてはいるものの、侵入型を含めたランサムウェア攻撃を決して対岸の火事とすることなく、万が一自組織で攻撃が発生した場合を想定して速やかに対策できるよう、是非とも攻撃を受ける前の段階で読み込んでおくことが望ましいでしょう。

- 例えば「Q1-2. 被害を受けたかどうか判断がつかないがどうしたらいいか？」では、ランサムウェアによる被害の発生を認識し得る一般的な状況(ファイルの拡張子が変わった、脅迫文が送られてきた、等)のみならず、ネットワーク内部での不審な探索、ファイルを外部へ送信する不審な通信等にも注意が必要としています。

- より早い段階でランサムウェアの存在・種別等を把握できるよう、侵入の検知はもちろん、いわゆる出口対策、そして可能な限り内部での不審な通信も検知できる機構の導入を検討すること、その後の侵害を受けたシステムやアカウントへの対応、バックアップの保護等についても迅速に対応できる体制を用意することが肝要です。

Impress Watch

JPCERT/CCが「侵入型ランサムウェア攻撃を受けたら読むFAQ」公開、相談窓口や初動対応の「3つの方針」など示す

山田 貞幸　2022年1月17日 20:05

[図1：侵入型ランサムウェア攻撃の特徴のイメージ]

一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）は、1月13日、侵入型ランサムウェアの被害に遭った企業や組織のCSIRTおよび情報セキュリティ担当を対象に、対応のポイントや留意点をFAQ形式でまとめた「侵入型ランサムウェア攻撃を受けたら読むFAQ」を公開した。

● 2021年に上場企業から個人情報流出は574万人分…東京商工リサーチ発表

https://www.itmedia.co.jp/news/articles/2201/17/news129.html
https://www.tsr-net.co.jp/news/analysis/20210117_01.html

このニュースをザックリ言うと・・・

- 1月17日(日本時間)、東京商工リサーチより、2021年に発生した上場企業(および子会社)の個人情報漏えい・紛失事故に関する調査結果が発表されました。

- 発表によれば、個人情報の漏えい・紛失事故の公表があったのは120社・137件で、漏えいした個人情報は5,749,773人分に上り、2012年以降の10年間で最多となるとのことです。

- 最も事故件数が多かった原因は「ウイルス感染・不正アクセス(事故68件、被害個人情報454,444件)」、次いで「誤表示・誤送信(事故43件、被害個人情報16,966件)」とされており、また被害を受けた個人情報件数では「紛失・誤廃棄(事故16件、被害個人情報32,818件)」が次点となっています。

AUS便りからの所感

- 漏えい・紛失件数が最多となったのはマッチングアプリ「Omiai」への不正アクセスによる1,711,756件で、他にも日本航空(JAL)と全日空(ANA)のマイレージ会員情報が、同じ会社が提供する管理システムへの不正アクセスにより、のべ約1,920,000件流出しています。

- 企業が上場する市場別の内訳で東証1部が97社(80.8%)と最多となっていることについては、「ガバナンスが徹底し、情報開示フローが充実していること」も背景にあるとしており、この調査結果に出ていない非上場企業が被害を受け、公表されてない事故が氷山の下に多く存在していると想像されます。

- 2020年の同様の事故が80社・103件であったのに比べそれぞれ3割近くの増加となり、それまでとは突出した規模となっていることが懸念される一方、事故の要因としては前述した3つが上位を占めており、過去に発生した事故を分析した上で、とるべき対策を今からでも確実に実行するよう心掛けることが重要です。

ITmedia NEWS

2021年、上場企業が漏えいした個人情報は574万人分 事故件数や社数は過去最多に

2022年01月17日 15時32分 公開　[松浦立樹，ITmedia]

「2021年に上場企業が漏えいした個人情報は574万人分に達した」――東京商工リサーチは1月17日、そんな調査結果を発表した。個人情報の漏えいや紛失事故を公表した上場企業（子会社を含む）は120社（前年比36.3%増）、事故件数は137件（同33.0%増）となり、2012年の調査開始以来、過去最多となった。

漏えい・紛失事故の年次推移（左）と、事故件数の内訳（右）

2021年に発生した事故で、漏えい・紛失件数が最多となったのは、ネットマーケティングが手掛ける、婚活マッチングサービス「Omiai」の不正アクセス事件で、171万1756件。次いでスイスの国際航空情報通信機構（SITA）への不正アクセス