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。

●楽天グループ管理の情報148万件以上、外部からアクセス可能な状態に…原因はクラウドサービスの設定不備

https://www.asahi.com/articles/ASNDT6F26NDTULFA03C.html
https://www.itmedia.co.jp/news/articles/2012/25/news161.html
https://www3.nhk.or.jp/news/html/20201225/k10012784641000.html
https://corp.rakuten.co.jp/news/update/2020/1225_01.html

このニュースをザックリ言うと･･･

- 12月25日(日本時間)、楽天より、同社およびグループ2社が保管していた個人情報等のべ148万件以上について、第三者からアクセスされた可能性があると発表されました。

- 被害を受けたのは、同社「楽天市場」の法人向け資料を請求した企業・店舗の名称・住所・代表者名・担当者名・電話番号・メールアドレス等最大1,381,735件、「楽天カード」の事業者向けローンを申し込んだ法人または個人事業主の情報・代表者および保証人の個人情報等最大15,415件、「楽天Edy」で故障した端末の残高移行サービスを申し込んだ個人氏名・端末の電話番号・Edy番号等最大89,141件とされています。

- 2016年1月以降、社外のクラウド型営業管理システムに保管されていた情報に外部からアクセス可能な状態にあったとされ、11月24日に外部からの指摘を受け同26日までに設定の変更を完了していますが、前述の情報のうち614件について海外からのアクセスが確認されたとのことです。

AUS便りからの所感等

- 管理システムについては楽天からの発表での明言はなかったものの、Salesforce社のサービスであることが報じられており、2016年にSalesforce側でデフォルトのセキュリティ設定が変更された後、楽天側で再設定を行っていなかったとされています(https://xtech.nikkei.com/atcl/nxt/news/18/09411/)。

- 多少異なるケースではありますが、社外ネットワーク上に構築していたデータベースサーバーに保存していた内部情報が、アクセス制限設定のミスで第三者からアクセス可能な状態にあったという事例も、例えば2019年7月に本田技研工業(AUS便り 2019/8/5号参照)において発覚しています。

- 大手企業からの個人情報流出が特に頻繁に報じられている昨今においては、ここで挙げた大規模なサービスから、小さいものではそれこそ個人のSNSやWebカレンダー等に至るまで、各種情報の公開・非公開設定を確実に行い、かつそれが適切に機能しているか確認することは肝要であり、また最初の一回だけ設定を行っていれば良いとするのではなく、サービス提供者からの設定変更等の告知に対しても適切に対応することが不可欠です。

NHK

楽天 システム不備 148万件の情報 不正にアクセスできる状態に

2020年12月25日 17時50分　IT・ネット

IT大手の楽天は顧客情報を管理するシステムに不備があり、個人情報を含む延べ148万件の情報が外部からアクセスできる状態になっていたと発表しました。このうち、600件余りの情報が海外から不正にアクセスを受けたことが確認されたということです。

発表によりますと、先月24日、「楽天」と子会社の「楽天カード」、それに「楽天Edy」の合わせて3社の顧客情報を管理するシステムに不備が見つかったと社外から指摘があったということです。

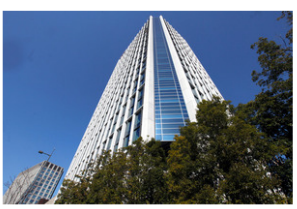
会社が調べたところ、「楽天市場」に出店する事業者の代表者や、ローンを申し込んだ事業者、それにスマートフォンなどが故障し、電子マネーの残高を別の端末に移すことを申し込んだ人の個人情報を含む延べ148万件の情報が外部から不正にアクセスできる状態になっていたということです。

朝日新聞 DIGITAL

楽天、事業者情報など148万件分流出か 「設定不備」

益田暢子　2020年12月25日 19時33分

シェア　ツイート　ブックマーク　メール　印刷



楽天本社=東京都世田谷区

楽天は25日、第三者からのアクセスで、楽天市場 に資料を請求した事業者や、楽天カードでローンを申請した事業者、電子マネー「楽天Edy」の一部ユーザーらの情報が最大148万件分流出した可能性があると発表した。2016年1月以降4年10カ月にわたり、外部から閲覧できる状態になっていたという。

第三者のアクセスが確認されたのは、楽天と同社の子会社2社が使う外部のクラウド型の顧客 情報管理 システム。楽天市場 の資料を請求した企業名や電話番号のほか、楽天Edyで端末が故障した際に残高が移せるサービスに申し込んだ利用者の名前や電話番号が保存されていた。

また、楽天カードのウェブサイトでローンを申請した法人や個人事業主の名前や 銀行口座 番号、運転免許証の番号、借り入れ状況、融資の審査結果などの情報もあった。

●「2020年の10大セキュリティ事件」、マカフィーが発表

https://kyodonewsprwire.jp/release/202012148607
https://www.mcafee.com/enterprise/ja-jp/about/newsroom/press-releases/press-release.html?news_id=2020121501

このニュースをザックリ言うと･･･

- 12月15日(日本時間)、セキュリティベンダーのマカフィー社より、同社がIT担当者等1,552人に対し実施した「2020年のセキュリティ事件に関する意識調査」に基づく「10大セキュリティ事件ランキング」が発表されました。

- 最も認知度が高かった事件は「携帯電話会社の電子決済サービスを通じて、利用者の預金が何者かに不正に引き出されたことが判明(9月)」で認知度59.2%に上り、次いで「ゲームメーカーが11月16日、サイバー犯罪集団からの不正アクセスを受け、顧客や取引先に関する情報が最大で35万件流出した可能性があると発表(11月)」が37.7%につけています。

- 以下、3位にはディープフェイクポルノ動画の公開容疑で2人が逮捕(36.5%)、4位に特別定額給付金に便乗した自治体等を騙るフィッシングサイト(35.4%)、5位に中国製動画投稿アプリTikTokの米海軍での使用禁止(35.1%)等、当AUS便りで取り上げたもの・取り上げられなかったもの含め、少なからず話題になった事件が取り上げられています。

AUS便りからの所感

- 同社が昨年発表した2019年のランキング(AUS便り 2019/12/23号参照)に続き、奇しくもモバイル決済サービスの不正利用事件が1位となっており、近年におけるQRコード決済等の爆発的な普及により、攻撃者が新旧の決済サービスの脆弱性に着目するようになった可能性が考えられます。

- この他、ネットサービスや企業ネットワークへの不正アクセス、企業の内部犯行による情報流出、そしてフィッシング等と、ランクインする事件の傾向も概ね2019年から引き続いたものとなっています。

- 年末年始には、大手セキュリティベンダーや関連団体等により、一年間に話題になったセキュリティ関連ニュースのまとめや、翌年における業界の動向予測等がリリースされますが、それぞれのランキングの内容は各組織の立ち位置・観点等の違いを少なからず反映したものとなっており、特にシステム管理者においては、各ランキングをはじめとしたセキュリティの脅威に関する情報収集を随時行うとともに、新しい脅威からの被害をも最小限に抑えられるようなシステム・ネットワークの見直しを随時検討して頂ければ幸いです。

順位	セキュリティ事件(時期)	認知度(%)
1	携帯電話会社の電子決済サービスを通じて、利用者の預金が何者かに不正に引き出されたことが判明(9月)	59.2
2	ゲームメーカーが11月16日、サイバー犯罪集団からの不正アクセスを受け、顧客や取引先に関する情報が最大で35万件流出した可能性があると発表(11月)	37.7
3	AIを使ってポルノ動画に写った人物の顔を芸能人の顔にすり替えた"ディープフェイクポルノ動画"を公開したとして、男性2人を名誉毀損と著作権法違反の疑いで逮捕(10月)	36.5
4	新型コロナウイルス感染症対策として10万円の特別定額給付金の給付が各自治体で始まるなか、自治体などのホームページを模倣したフィッシングサイトが相次いで確認(5月)	35.4
5	米海軍はサイバーセキュリティ上の懸念を理由に、政府支給のモバイルデバイスで中国製アプリ「TikTok」を使用することを禁止した(2019年12月)	35.1
6	総合電機メーカーがサイバー攻撃を受け、個人情報や機密情報が流出したおそれがあると発表(1月)	33.5
7	総合電機メーカーへのサイバー攻撃で、防衛関係の機密情報が同社から漏えいした疑いがあることが判明(5月)	32.9
8	納税などに関する大量の個人情報や秘密情報を含む地方自治体の行政文書が蓄積されたハードディスク(HDD)が、ネットオークションを通じて転売され、流出していた(2019年12月)	31.4
9	「Zoom」の「Windows」版クライアントについて、攻撃者がグループチャットのリンク共有機能を悪用した場合、リンクをクリックした人のWindowsのネットワーク認証情報が漏えいする可能性があることが明らかに(4月)	30.9
10	電気通信事業者等を傘下に置く特殊会社の機密情報を不正に取得したとして、同社元社員を逮捕。容疑者が取得した機密情報は在日ロシア通商代表部の職員らに譲渡されたとみられる(1月)	30.2

●Emotet、12/21から活動再開…IPA注意喚起

https://www.ipa.go.jp/security/announce/20191202.html#L14
https://twitter.com/IPA_anshin/status/1341327522336628736

このニュースをザックリ言うと･･･

- 12月22日(日本時間)、IPAより、マルウェア「Emotet」の活動が同21日から再開されたとして注意喚起が出されています。

- Emotetは10月末以降活動を休止していましたが、今回「クリスマス」「賞与支給」等のキーワード、年末の時期に合わせたとみられる件名・添付ファイルでのメールの拡散が確認されているとのことです。

- 現時点でのEmotetに感染させる手口は、これまでと同様に「Word文書ファイルのマクロ機能の悪用」とされている一方、今後も攻撃は継続すると考えられ、引き続き警戒するよう呼び掛けられています。

AUS便りからの所感

- JPCERT/CCからも同様の注意喚起(https://www.jpcert.or.jp/newsflash/2020122201.html)が出ている他、内閣サイバーセキュリティセンター(NISC)によれば、Emotetと類似した手口をとるとされる別のマルウェア「IcedID」(AUS便り 2020/11/09号参照)についても報告が増えているとのことです(https://www3.nhk.or.jp/news/html/20201226/k10012785331000.html)。

- 年明け以降も、年始の挨拶等を騙ったマルウェア添付メールが拡散するのは確実とみられ、IPA等が随時更新する情報をチェックし対応していくことが大切です。

- Emotetが恐ろしいのは「感染したPCに保存されている送受信メールのアドレス・文面を悪用して、マルウェア添付メールを送信する」手口もとることであり、日頃メールのやり取りをしている取引先等からのメールであっても決して油断することなく、慎重に行動するよう努めましょう。


「Emotet」と呼ばれるウイルスへの感染を狙うメールについて

最終更新日：2020年12月22日
独立行政法人 情報処理推進機構
セキュリティセンター

年末時期に合わせた攻撃の再開（2020年12月22日 追記）

Emotetの攻撃メールについて、2020年10月末から観測されない時期が続いていましたが、2020年12月21日から、年末の時期に合わせたような件名・添付ファイル名での攻撃を確認しました。具体的には「クリスマス」や「賞与支給」といったキーワードが使われているとの情報があります。

図11 「メリークリスマス」という攻撃メールの例（2020年12月）