

コラム記事

新型コロナウイルスの拡大により、リモート勤務とする企業が増えている中、リモート接続の脆弱性を狙ったサイバー攻撃も増加しています。

1人1人のサイバー攻撃に対するセキュリティー知識の向上により、従来のようにメールに添付されているファイルを開いて感染するようなサイバー攻撃ではなく、目に見えない環境下での攻撃が増加しています。

1度ウイルスの侵入を許してしまうと、データへのアクセスが制限（もしくは不可能）され、代金の要求をされるケースも報告されています。

特に病院のように、多くの個人データを長期間保持し続ける可能性があるような企業であれば、なおさら侵入を許さない対策が必要不可欠です。

最新のセキュリティー知識を持つこと、多様化するサイバー攻撃に対応するセキュリティーソフトを導入することが各企業での喫緊の課題となっており、セキュリティー対策が急務になっていると感じています。

そんな中、下記記事が掲載されていたのでご紹介いたします。



大阪急性期・総合医療センターでシステム障害 サイバー攻撃か

(NHK NEWS WEB 2022/10/31(月) 22:35 配信 より引用)

大阪 住吉区の大阪急性期・総合医療センターは「ランサムウェア」と呼ばれる身代金要求型のウイルスによるサイバー攻撃を受け、電子カルテのシステムに障害が発生して緊急以外の手術や外来診療などを停止していると発表しました。復旧のめどは立っておらず、11月1日以降もこの状況が続くとしています。

これは31日、大阪急性期・総合医療センターが記者会見を開いて明らかにしました。

病院によりますと31日午前7時ごろ、電子カルテのシステムに障害が発生し閲覧などができなくなりました。

業者に相談して調査したところ、システム障害の原因は「ランサムウェア」と呼ばれる身代金要求型のウイルスによるサイバー攻撃を受けたためとみられるということです。

病院のサーバーには「すべてのファイルを暗号化した。復元のためにはビットコインで支払え。金額はあなたがどれだけ早く、われわれにメールを送るかによって変わる」という英文のメッセージが届いたということです。

病院は31日朝から緊急以外の手術や外来診療などを停止しています。

今のところ復旧のめどは立っておらず、現在は紙のカルテを作成するなどして対応していますが、11月1日以降も通常の診療ができない見通しだということです。

大阪急性期・総合医療センターの嶋津岳士総長は「現在、原因の究明とシステムの復旧に向けて努力をしている。患者さん

をはじめ、関係者の皆様に多大なご心配とご迷惑をおかけしてしまい誠に申し訳ありません」と話していました。

大阪急性期・総合医療センターは36の診療科に865のベッドがある総合病院で救急やがんなどの診療で地域の拠点となっています。

●「ランサムウェア」とは 医療機関で被害相次ぐ

身代金要求型のコンピューターウイルス「ランサムウェア」は企業や組織などのサーバーに保管されたデータなどを暗号化し、アクセスできなくした上、暗号化の解除を引き換えに金銭を要求するサイバー攻撃の一つです。

侵入経路としては、不特定多数にメールを送りつけた上、添付ファイルや本文に書かれた URL でダウンロードさせる方法などがあるほか新型コロナウイルスの影響で利用が広がっている「VPN」などのリモート接続の脆弱性をねらうケースも目立っています。

医療機関が被害を受けた「ランサムウェア」によるサイバー攻撃は、国内では2018年に奈良県宇陀市の市立病院で患者の一部の診療記録が見られなくなるなどの影響が出たほか、去年は、徳島県つるぎ町の町立病院で電子カルテや会計システムのデータなどが暗号化され、およそ2か月にわたり、産科などを除いて新規患者の受け入れを停止する事態となりました。

この病院のケースでは、バックアップ用のサーバーもウイルスに感染し、患者の検査結果やX線などの画像が参照できなくなり、処方した薬の記録も見られない状態が長期間続き、診療に大きな支障がでました。

さらに、ことしに入ってから1月に愛知県春日井市の病院がおよそ5万人の患者の情報が記録された電子カルテにアクセスできなくなるなどの被害が出ています。

こうした事態を受け、厚生労働省は医療機関向けのセキュリティー対策のガイドラインを改定し、バックアップの在り方や被害に遭った時の速やかな対処など「ランサムウェア」への対策を喫緊の課題として挙げています。

(カンテレ 2022/11/7(月) 23:28 配信 より引用)

サイバー攻撃を受けた大阪急性期・総合医療センターは、システムの完全復旧が来年1月になる見通しを明らかにしました。

大阪急性期・総合医療センターは10月31日、身代金要求型のウイルス「ランサムウェア」のサイバー攻撃によって大規模なシステム障害が発生し、現在も外来診療などを停止しています。

センターは7日夜、会見を開き、システム障害の完全復旧は来年1月を見込んでいることを明らかにしました。

一方で電子カルテのバックアップデータを活用できる環境を10日をめどに整え、順次手術や外来診療の受け入れを拡大する方針です。

また、給食を委託する堺市の業者でもシステム障害が起きていたことが分かり、この業者のサーバー経由でランサムウェアに感染した可能性が高いということです。



ご紹介した通り、ランサムウェアによるサイバー攻撃は年々増加しており、復旧まで時間がかかる場合が多くあります。情報を守るためはもちろんですが、システム復旧に向けた営業停止リスク回避のためにもサイバー攻撃に対する知識とセキュリティーソフト情報の共有については、各企業において非常に重要な課題であると感じています。