2023 年 3 月 16 日

Venture Solution

コラム記事

新型コロナウイルスの拡大により、テレワークを推奨する企業が多くなってきています。
テレワークに関しては、場所を問わず仕事が出来ると言うメリットもありますが、
その反面、高頻度でセキュリティの脆弱性について指摘される場面があるように感じております。
そこで、ランサムウェア被害の実情とテレワークの関連性についての記事が掲載されておりましたので
ご紹介いたします。

身代金要求「ランサムウェア」被害 1.5 倍に データ公開で「二重脅迫」65% テレワーク定着の影響も

（FNN プライムオンライン 2023/3/16(木) 10：07 配信 より引用）

警察庁は、去年 1 年間に、全国の警察が摘発したサイバー犯罪の傾向などについて発表した。身代金要求型ウイルス「ランサムウェア」による被害が 230 件にのぼり、身代金を払わないとデータを公開すると脅す「二重恐喝」が半数を超えたという。

警察庁によるとサイバー犯罪のうち、機密情報のデータを暗号化して、復旧と引き換えに金銭を要求する「ランサムウェア」の被害は、230 件にのぼった。おととしから、およそ 1.5 倍増えた。

手口が確認できた 182 件のうち、金銭要求に応じなければ、データを暴露するなどと、さらに脅す「二重恐喝」の手口が 119 件にのぼり、全体の 65%を占めた。

（FNN プライムオンラインより引用）

被害は、大企業から中小企業や団体など規模を問わず発生し、業種別では、製造業が最も多い 75 件、サービス業が 49 件、医療、福祉が 20 件などだった。

感染経路がわかった被害のうち 8 割以上がテレワークなどに利用される（仮想プライベートネットワーク=VPN）機器の脆弱性や、盗まれやすい認証情報などが狙われたとみられる。

被害を受けた企業では生産や販売停止を余儀なくされ、医療機関では電子カルテシステムの障害で手術や診療が一時停止するなど多大な影響があり、警察庁は、関係機関と連携してセキュリティ対策の強化を呼びかけている。

警察庁による発表となるため信頼のおける数字ですが、警察庁の発表=被害届のあった数と考えねばならず、実際には「被害にあっていることさえ気づいていない」ケースも多々あると考えなければいけません。

実態としてはこの件数の数倍～数十倍発生している可能性もあります。

注目に値する点は感染経路の 8 割以上が VPN や認証技術の脆弱性を利用されているという点です。

ランサムウェア対策として端末のセキュリティ強化として EDR 等が検討されることが多いのですが、EDR は侵入後の影響調査等に効果を発揮する傾向が強く、侵入予防という観点ではリモートアクセスや認証技術の強化が重要です。