セキュリティ分析結果レポート

INJANET 株式会社

お客様：　Xxxx クリニック様　　報告日：　2020/10/10

分析実施内容

① 情報資産の洗い出し
8 件(8 種類)の試算を洗い出しました

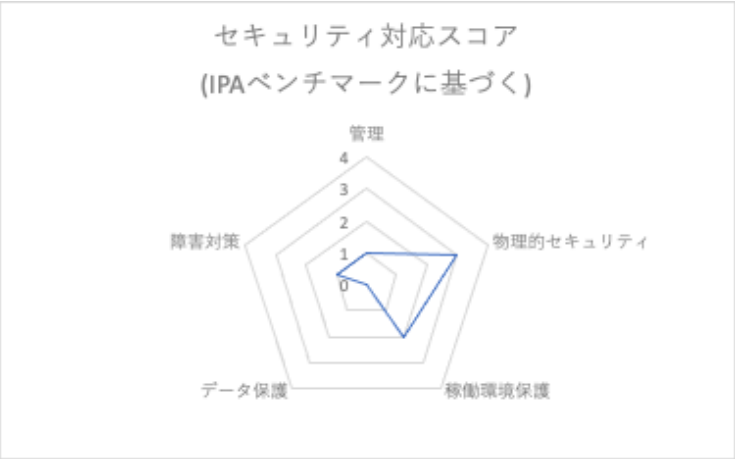
② リスク分析
リスク値が高い試算と攻撃ルートは、
・WiFi アクセスポイントからの侵入
・事務用 PC で不審メールを開くことによるランサムウェアの攻撃

③ 分析に基づくセキュリティ対策
・WiFi アクセスポイントの設定を固めました
・アンチウィルスの更新を行いました

④ 推奨対策候補のご紹介
LAN ブレーカを使って重要なサーバを切り離す事を推奨いたします。

分析結果外用

セキュリティ対応スコア

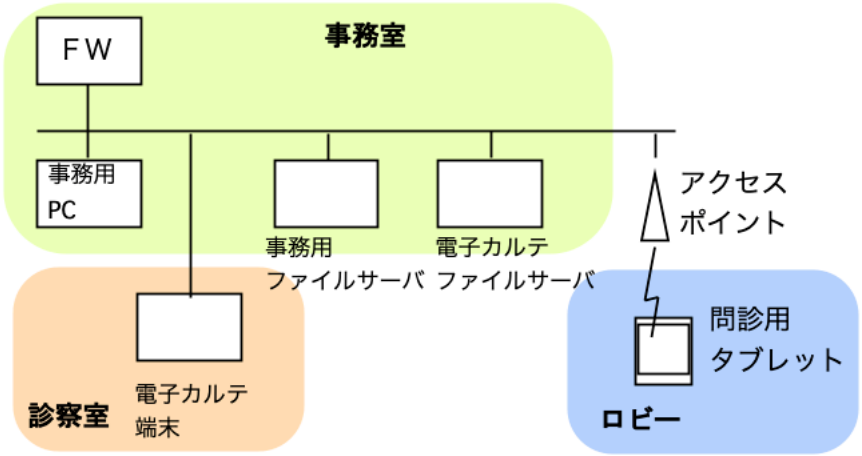


総評：的確なセキュリティ対策が出来ていますが、一部抜けのあった所が見えました。
また、院内でのトレーニングが十分では無いようです。定期的にスパムメールやランサムウェア被害発生時対応のトレーニングを行う事をお勧めします。

結果詳細：

① 情報資産の洗い出し

ヒアリングにより以下のシステム構成図を作成しました。(類似資産はまとめています)



＊電子カルテサーバのセキュリティ対策は不明

資産一覧表

	G	H	I	J	K	L	M	N	O	P
1			出力するファイル名							
2			XXXクリニック							
3		No.	1	2	3	4	5	6	7	8
4		資産ベースシート生成	更新	更新	更新	更新	更新	更新	更新	更新
5		資産名	FW	院内LAN	事務用PC	事務用ファイルサーバ	電子カルテサーバ	アクセスポイント	電子カルテ端末	問診用タブレット
6	資産種別	機器/NW機器/NW種別	NW機器	NW	機器	機器	機器	機器	機器	機器
7	物理進入	USB/LANポート/無線	v		v	v			v	
8	論理進入	ネットワーク接続	v					v		
9	セキュリティ対策	ファイアウォール（パケットフィルタ）			v					
10		ファイアウォール（AG）								
11		一方向GW								
12		プロキシサーバ								
13		IPS／IDS								
14		DDoS対策								
15		通信相手の認証					v		v	
16		専用線								
17		通信暗号化								
18		アンチウィルス			v				v	
19		WAF								
20		URLフィルタリング/Webレピュテーション								
21		メールフィルタリング								
22		APT対策ツール								
23		パッチ適用			v					

② リスク分析結果

リスクが高いと分析されたのは以下の２点です。

a. 事務用ＰＣがフィッシングメールを受け取り電子カルテサーバが暗号化や情報漏えいの被害を受ける可能性があります
b. WiFi スポットを侵入口として、院内ＬＡＮに侵入される可能性があります。

③ 想定されるサイバー攻撃

・「見積書」と記載された取引先からのメール添付のマクロを開きマルウェア感染。バックドアを設置され、インターネット側からＰＣを操作し、電子カルテサーバの情報を窃取。のちに暗号化し脅迫する。請求額の相場 xxxx 万円(2020 上期平均)。

・WiFi スポットから侵入し内部のＬＡＮを調査されマルウェアを移植される。その後は上記と同様。

④ 実施した対策

a. 事務用ＰＣのアンチウィルスのパターンファイル更新が止まっていたので、動作するよう設定しました。また、事務用ＰＣと電子カルテサーバの利用者アカウントを別のものに設定しました。この対策により、攻撃者が電子カルテサーバを攻略するのは難しくなります。
b. WiFi の設定を変更しました。元々弱いプロトコル(WEP)を利用されていたものを強いもの(WPA2)に変更しました。同時にアクセスポイントのファームウェアを脆弱性回避のためアップデートしました。

⑤ 今後推奨される対策

・院内を事務用 LAN と医療用 LAN を分離してファイアウォールなどでセグメント分割をするのが良いでしょう。(具体例 yyyy)

・さらに UTM を導入して不審なデータを通さないようにする事も良いと思います。(具体例 yyyy)

・ファイルではなく、メモリのみで動作するマルウェアはお客様のアンチウィルスでは検出できません。事務用ＰＣにホワイトリスト型のアンチウィルス（具体例 yyy）を入れるか、ＥＤＲ型のアンチウィルス(具体例 yyy)を導入するのも良いと思います。

弊社ではインストール、セットアップ等の作業も承っています。