静岡県防犯責任者専門セミナー質問・意見要望書

	内容	回答
質問内容	一般的なランサムウェアの定義がわかりにくいです。 人質となるファイルを暗号化しなくても、盗み出したファイルをで身代金を 要求されるマルウェアであれば、ランサムウェアとみなしても良いでしょうか。 ランサムウェア＝暗号化のイメージが強い為、ランサムウェアをどのように 説明するのが適切なのかを教えて頂けると大変助かります。	暗号化されなくても盗んだ情報を公開するぞ！というのも ランサムウェアです
	静岡県内での災害件数と被害額と事例を知りたい。	令和5年上期で103件、金額は公開されていません。 詳細は下記で公開されています https://www.pref.shizuoka.jp/police/kurashi/bohan/cyber/zyosei.html#:~:text=%E9%9D%99%E5%B2%A1%E7%9C%8C%E5%86%85%E3%81%AB%E3%81%8A%E3%81%84%E3%81%A6%E3%82%82%E3%80%81%E7%99%BA%E7%94%9F,%E5%A4%9A%E6%95%B0%E7%A2%BA%E8%AA%8D%E3%81%95%E3%82%8C%E3%81%A6%E3%81%84%E3%81%BE%E3%81%99%E3%80%82
	現在システム担当を行っています。 サイバー攻撃への対策について勉強したいと思っておりますのでよろしくお願いいたします	よろしくお願いします
	#1　専門知識が乏しいので、知識の初歩的段階から、ご教授頂きたいと考えます。 #2　ランサムウェアに係る報道から、Ｅメールの添付ファイルを開封するとウィルス 感染、と見聞きします。そこで質問ですが、Ｅメールを見出し一覧表からクリック する段階ではまだ感染とは言えないのか、ウィルス感染ファイルを持つＥメールを 選んだ時点で、もう既に感染し始めているのか、ご教授下さい。 #3　昼食後の睡魔や夜間残業の睡魔、等うっかりがきっかけで、ウィルスメール誤開封 してしまった場合の措置を教えて下さい。「解毒剤」なるワクチンもどきの処理は あるのでしょうか。 #4　一旦にウィルス感染した場合には、事業所のランも感染していると捉えるべきで しょうか。その場合には、事業所のＰＣ含めて全廃棄になるのでしょうか。	添付ファイルの開封のタイミングで感染するのが一般的です まれに見ただけで感染する場合もあるようです 対策としては、メールの表示をHTMLではなくテキスト形式で 表示する方がセキュリティ的には効果があります https://support.microsoft.com/ja-jp/office/%E3%83%A1%E3%83%83%E3%82%BB%E3%83%BC%E3%82%B8%E5%BD%A2%E5%BC%8F%E3%82%92-html-%E3%83%AA%E3%83%83%E3%83%81-%E3%83%86%E3%82%AD%E3%82%B9%E3%83%88%E5%BD%A2%E5%BC%8F-%E3%81%BE%E3%81%9F%E3%81%AF%E3%83%86%E3%82%AD%E3%82%B9%E3%83%88%E3%81%AB%E5%A4%89%E6%9B%B4%E3%81%99%E3%82%8B-338a389d-11da-47fe-b693-cf41f792fefa 感染の可能性が確認された場合、そのPCをネットワークから すぐに分離することが重要です ネットワーク状のすべてのPCが感染するかはマルウェアの種類等によって異なります 感染した場合、大抵はPCの初期化で直る可能性があります ただ、BIOS等に影響を与えた場合は廃棄になるかもしれません
	ゼロデイ攻撃等明確な事前対策が難しいものの対応として他企業、他業種の方達がどのようにしているか情報があったりしますか？	サンドボックスの導入が効果があると思います。 (サンドボックスとは企業のユーザーが通常利用する領域から隔離され、保護された空間に構築された仮想環境のことです。) https://eset-info.canon-its.jp/malware_info/special/detail/201117.html
	緊急事態対応計画の作成、サイバーセキュリティテスト(サイバーアタックのシミュレーション)の実施方法など参考になるものがあればご教示願います。	緊急時の対応計画はBCP策定の中で考えるのはどうでしょうか？ サイバーセキュリティ関連の訓練等のサービスがあります。 https://jpn.nec.com/cybersecurity/service/professional/education/training/index.html
	今回のセミナーでは、代表的なネットウイルスについて説明をしてくださりましたが、ウイルス以外にもワームなどほかの種類の対策などはどうすればよいでしょうか？	基本的にエンドポイントの対策（ウィルス対策ソフトの導入）で 対応できると思います。
	現在の主流なサイバー攻撃について、具体的に事例をあげた説明で、理解を深めることができました。 ・実際に、県や日本の単位での各種攻撃に対する件数はどのように推移しているのでしょうか。 ・対策について、メールを不用意に開かない事や、社内ルールつくり、徹底等の組織教育の醸成や、システムの最新化が基本となるかと思いますが、具体的な改善の成功例等はありますでしょうか。	国の件数は下記で公開されています。 https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r04/html/nd237200.html 静岡県の件数は下記で公開されています。 ここで公開されています https://www.pref.shizuoka.jp/police/kurashi/bohan/cyber/zyosei.html#:~:text=%E9%9D%99%E5%B2%A1%E7%9C%8C%E5%86%85%E3%81%AB%E3%81%8A%E3%81%84%E3%81%A6%E3%82%82%E3%80%81%E7%99%BA%E7%94%9F,%E5%A4%9A%E6%95%B0%E7%A2%BA%E8%AA%8D%E3%81%95%E3%82%8C%E3%81%A6%E3%81%84%E3%81%BE%E3%81%99%E3%80%82 成功した！と感じることはあまりないと思います。 おっしゃるような地道な対策を継続するのが効果的だと思います。
	ランサムウェア被害にあった場合、身代金を払った場合復旧する確率が思っていたよりも高いという結果が示されておりましたが、実際に支払った身代金の平均額や身代金を支払わずに復旧に要した費用の平均額などのデータはありますでしょうか。	少し古いデータですが平均1億円程度と言われています。 https://japan.zdnet.com/article/35162969/
意見・要望	サイバー攻撃を受けた時の対応や相談について、警察や官庁等への連絡先や各窓口の電話番号を詳しく教えていただきたいです。	原則、最寄りの警察署に届けることになります。
	静岡県として、サイバーセキュリティ対策の共同実施等ができる枠組みがあればご紹介頂きたいです。	静岡県中小企業サイバーセキュリティ支援ネットワーク https://www.pref.shizuoka.jp/police/kurashi/bohan/cyber/network.html
	事例を多く共有いただき、勉強になりました、ありがとうございました。 対策についても、自分ごと化できる内容、例えば、メールやVPN機器によるリスク顕在化事例が多いが、より安心安全にこれらを活用できる方法やメール以外のおすすめのコミュニケーションツールなど、もしあればお聞きしたかったです。	メール以外のコミュニケーションとなると 社内ではグループウェア 社外ではセキュアなコミュニケーションツールの活用がよろしいかと 例えばSIGANL https://nordvpn.com/ja/blog/signal-app-security/