情報セキュリティマネジメント試験対策動画。。。今回のテーマは、2024年10月から適用される新シラバスで追加される用語です。

セキュアバイデザイン。。。

システム開発の後段でセキュリティ対策を講じるのではなく、システムの企画や設計の初期段階から考慮し、対策を盛り込む考え方のことです。セキュアバイデザインの導入にあたって、以下5点が推奨されています。。。

1。メモリ安全性を備えたプログラミング言語の採用。。。

2。アプリケーションセキュリティのテスト実施。。。

3。コードレビューやソフトウエア部品表、えすぼむの採用。。。

4。脆弱性の報告を奨励する開示プログラムの導入。。。

5。侵害をシステム全体に広げないための多層防御の導入

えすぼむ。ソフトウェアビルオブマテリアルズ。。

ソフトウェアに含まれる材料をリストアップしたソフトウェア部品表のことです。OSS、オープンソースソフトウェアのライセンス管理や脆弱性の管理、ソフトウェアサプライチェーンのリスク管理等の用途で利用されています。このひょうのような作りがエスボムとなります。

らっと。リモートアクセスとろーじゃん。。

リモートアクセス型トロイの木馬、らっとは、攻撃者が感染したコンピューターをリモートで制御できるように設計されたマルウェアです。侵害されたシステムでらっとが実行されると、攻撃者はらっとにコマンドを送信し、それに応じてデータを受信することができます。

ファイルレスマルウェア。。

パソコンのOSに組み込まれた正規のツールや機能を悪用する攻撃のことです。ファイルがディスクじょうに保存されるのではなく、メモリじょうに書き込まれて動作するため、従来のアンチウイルスソフトでは検知が難しいという特徴があります。

割れ窓理論。。

建物の窓が壊れているのを放置すると、誰も注意を払っていないという象徴となり、他の窓もまもなくすべて壊されてしまう傾向が高いという事実から、反対に割れた窓をすぐに修理すれば、他の窓が割られる確率は低くなるというアメリカの犯罪学者ジョージケリング博士が提唱した理論のことです。

防犯環境設計。。

犯罪が発生しにくい環境を創るために、人的な防犯活動、ソフト面とあわせて、建物、道路、公園等の物理的な環境、ハード面の整備、強化等を行い、犯罪の起きにくい環境を形成するという考え方のことです。。

防犯環境設計には、直接的な手法として対象物の強化と接近の制御、間接的な手法として監視性の確保、領域性の確保があり、これらを総合的に組み合わせることが重要とされています。

二重脅迫。ダブルエクストーション。。

通常のランサムウェアは被害者のデータを暗号化して、復号化ツールと引き換えに支払いを要求しますが、二重恐喝は、被害者のデータを暗号化し身代金の支払いも要求しますが、さらに被害者のデータを暗号化前にコピーしておき、そのデータをオンラインで公開しないようにするための支払いも要求します。最近流行りのやつですね。

リークサイト。。

暴露型ランサムウエア攻撃グループが攻撃声明を公表したり、交渉が決裂したときにデータを公開したりするのに用いる呼ばれるWebサイトのことです。その多くが、通常のWebブラウザではアクセスできないダークウェブに存在します。

クレデンシャルスタッフィング攻撃。。

盗まれたアカウント資格情報でWebアプリケーションなどのサービスに大規模な自動ログイン要求をおこなうことで、ユーザアカウントへの不正アクセスを試みる攻撃の一種です。アカウント資格情報は通常、ユーザ名や電子メールアドレスと対応するパスワードリストで構成されます。クレデンシャル、つまり認証情報を使いスタッフィング、総当たり的に検証することからクレデンシャルスタッフィング攻撃と呼ばれます。クレデンシャルスタッフィング攻撃はロボットが行い、パスワードリスト攻撃は手動で行うのが異なる点です。

OSコマンドインジェクション。。

Webサーバへのリクエストの中に不正なOSコマンドを注入することで、Webサーバ側に意図しない不正な命令を実行させる攻撃手法のことです。

オープンリレー。第三者中継。。

メール送信サーバ、SMTPサーバが、外部からの送信依頼を受け付けることです。特に、何の制限も無く誰でも自由にメールを送信できるよう開放している状態をさします。迷惑メールやウイルスメールの送信に悪用されるため好ましくないとされています。

らーす。ランサムウェアアズアサービス。。

ランサムウェア本体や身代金要求のためのインフラなどランサムウェア攻撃に必要ないっしきをサービスとして提供するものであり、サイバー犯罪のビジネスモデルのひとつです。らーすが登場したことで、技術的な知識を持たないサイバー攻撃者でも自分たちが狙う対象に対して容易にランサムウェア攻撃を仕掛けることが可能になりました。これも最近とても流行ってますよね。

ラテラルムーブメント。。

外部の攻撃者やマルウェアが企業の内部ネットワークの侵入に成功したあと、ネットワークないを横移動し侵害範囲を拡大していく攻撃手法のことです。ラテラルムーブメントが成功すると、侵害範囲が拡大するだけでなく、より重要なシステムや機密性の高いデータが狙われてしまいます。また、攻撃者は一般的なセキュリティ対策を潜り抜けるように攻撃を進めるため、攻撃の進行を検知しにくく、判明した時には既に大きな被害が生じている場合があります。怖いですね

しゃーつー。セキュアハッシュアルゴリズムつー。。

しゃーつーはNSA、米国家安全保障局が考案し、2001年ににすと、米国標準技術局によって連邦情報処理標準のひとつとして標準化された暗号化アルゴリズムのことです。しゃーにーにーよん、しゃーにーごーろく、しゃーさんはちよん、しゃーごーいちにーの4種類があり、これらの末尾の数字が、それぞれが出力するハッシュ値のビット長を表しています。最長のしゃーごーいちにーが最も安全性が高いが、一般的にはSHA-256が最もよく利用されています。

メッセージダイジェスト。。

元のデータを要約した短いデータ、ハッシュちのことです。メッセージダイジェストから元のデータを逆生成できない、元のデータが1文字でも変わればメッセージダイジェストも全く異なる値に変わるという特徴があり、送信前のメッセージダイジェストと、送信後のメッセージダイジェストを比較することで、データが改ざんされていないことを保証します。

トラストアンカー。信頼のきてん。。

HTTPS通信における、OSやブラウザベンダが提供するソフトウェアに登録されている認証局が発行したルート証明書を指します。インターネットじょうのやり取りは、通常不特定多数の相手と行います。その中でトラストアンカーと認証局は、顔の見えないインターネットの通信に、何かしらの信頼を与える機能を実現します。

中間しーえー証明書。。

証明書を発行する認証局の実在を認証するための証明書のことです。ルートしーえー証明書からの認証パスを構築するため、証明書を発行する認証局の上位の認証局が発行します。中間しーえー証明書は、サーバ証明書と共にWebサーバにインストールする必要があり、通常、証明書を発行した認証局から入手します。

サイバーハイジーン。。

ハイジーンとは、衛生を表す言葉で、IT環境がウイルスに汚染されないための予防対策として必要な衛生管理という意味です。セキュリティパッチの速やかな適用、サイバー攻撃対策ソフトの導入やパスワードの強化、不正アクセスを防ぐためのセキュリティソフトの使用などが挙げられます。

地政学的リスク。ジオポリティカルリスク。。

特定の地域の政治的、軍事的、社会的な緊張の高まりが、周辺地域や世界の経済の先行きを不透明にするリスクのことです。紛争やテロによって石油関連価格が値上がりして業績が悪化したり、世界経済が停滞したりすることなどが挙げられます。

ぴーさーと。ぷろだくとさーと。。

自社が製造、販売した製品の安全確保のため、製品の安全性を脅かす外的脅威に対するセキュリティ対応を専門に実施する組織のことです。製品の開発ライフサイクルにおけるセキュリティ脆弱性に関わるリスクマネジメントや、セキュリティインシデント発生時の有事対応を行います。しーさーととの違いについて、このイラストにまとめてみました。しーさーとは、おもに社内ネットワークなどに対して被害を最小化するためにサポートすることが目的となっています。一方ぴーさーとは、先ほどの説明の通り、自社が製造、販売した製品に対するサポートが目的となっております。この違いをイラストでイメージを固めてください。

あいざっく。インフォメーションシェアリングアンドアナリシスセンター。。

業界内での情報共有、連携の取り組み推進を図る組織のこと。国内では金融あいざっくや交通あいざっく、電力あいざっくなどが存在する。セキュリティ情報共有組織とも呼ばれます。

ノーティス。。

総務省、国立研究開発法人情報通信研究機構、にくと。インターネットサービスプロバイダ、ISPが連携し、あいおーてぃー機器のセキュリティ対策向上を推進することにより、サイバー攻撃の発生や、その被害を未然に防ぐためのプロジェクトのことです。あいおーてぃー機器の安全な管理方法の広報や、危険性があるあいおーてぃー機器の管理者、利用者への注意喚起を行っています。

エシカルハッカー。。

コンピュータやソフトウェアのシステムまたはプロセスをテストし、セキュリティを評価、強化、改善することを専門とするセキュリティ専門家のことです。

エシカルハッカーには、レッドチーム、ブルーチーム 、バグハンター、ペネトレーションテスターなどの種類が存在します。

セキュリティクリアランス。。

政府が保有する安全保障上重要な情報として指定された情報にアクセスする必要がある者に対し、その者の信頼性を調査、確認した上でアクセスを認める制度のことです。機密情報にアクセスできる人を限定することで、その情報の漏洩を防ぐことがおもな目的です。

わーむ。らいとわんすりーどめにー。。

一度書き込んだデータを消去、変更できない追記型の記憶方式のことです。操作ミスや故意によるデータの改ざん、削除を防ぐことができるため、コンプライアンス対応やセキュリティの強化に有効です。

3、2、1ルール。。

組織がデータをバックアップする際に推奨されているルールです。常にみっつのデータコピーを作成し、それらをふたつの異なる媒体に保管し、ひとつは別の場所に保管するという方法のことです。ランサムウェア攻撃の増加に伴い、組織のデータ復旧が喫緊の課題となっており、3-2-1ルールなどの実践が求められています。

データマスキング。。

元のデータ構造や意味を保持しつつ、特定の情報を非表示、書き換え、変更することで、データの機密性を保護する技術のことです。使用状況や要件に応じて置換、シャッフル、ハッシュ化、暗号化などの手法が選択されます。

暗号化消去。クリプトグラフィックイレース。しーいー。。

サーバなどに暗号化して保存したデータが不要になった際、当該データを削除すると同時に暗号化に使用した鍵を削除することで、データ抹消処理に置き換え利用不能にする論理的な削除方法のことです。オンプレミスやクラウドサービス利用において、削除対象のデータに機密情報や機微情報が含まれていた場合にデータ消去が課題でしたが、暗号鍵を消去することで復元が不可となり、第三者への情報漏えいを防止できるようになりました。

AIふぉーセキュリティー。AIを使ったセキュリティ技術。。

情報セキュリティの分野で人工知能、AI技術を利用することを指します。これには、サイバーセキュリティ、物理的セキュリティ、データ保護、アクセス制御など、様々なセキュリティの側面が含まれます。

セキュリティふぉーAI。AIそのものを守るセキュリティ技術。。

AIシステムの設計、開発、運用においてセキュリティ面を強化するための一連の対策や戦略を指します。

EDR。エンドポイントディテクションアンドレスポンス。。

エンドポイント、PC、サーバー、スマートフォン、タブレットなどネットワークに接続されている端末の操作や動作の監視を行い、サイバー攻撃を検知し次第対処するソフトウェアの総称です。マイクロソフトのディフェンダーフォーエンドポイントや、サイバーリーズンなどが有名です。

Webアイソレーション。。

ブラウザ分離とも呼ばれ、Webサイトの閲覧活動をエンドポイントから切り離し、悪意のあるコードやマルウェアなどからユーザを守る技術のことです。Web分離技術を使うことで、Webサイトを経由したブラウザやPCへの攻撃を防止することができます。アイソレーションは、分離という意味です。

セキュリティゾーニング。。

企業などで、部署内のセキュリティを確保する際に使われる方法です。来訪者や一般従業員、機密にアクセスできる担当者など関係者を明確に区分けし、入室可能なエリアを厳密に設定して重要な情報に権限の無い者がアクセスするといったことを防ぎます。

ベイジアンフィルタリング。。

ベイズの定理を応用してデータを分類、予測する方法のことです。特にスパムメールの検出やリコメンデーションシステムなどに広く利用されています。また、学習機能を持っており、多量のデータ分類をこなすことで、その精度を高めることができます。

送信元ドメイン認証。。

電子メールの送信元ドメインが実際にそのドメインを所有または管理している組織によって使用されていることを確認するための技術的な手法のことです。これにより、スパムメールやフィッシングメールを防ぐことができます。代表的な手法として、SPF、でぃーきむ、でぃーまーくがあります。

イラストを見ながらお聞きください。。

でぃーまーく。どめいんべーすどメッセージオーセンティケーション、レポーティングアンドこんふぉーまんす。。

電子メールの送信元ドメインを認証するためのプロトコルです。SPFおよびでぃーきむと連携して動作し、受信者が送信元のメールドメインについての信頼性を評価しやすくします。また、でぃーまーくは認証結果に基づいて受信したメールをどのように処理するかをポリシーとして指定し、そのポリシーに基づいて行動する仕組みを提供します。

このイラストをイメージして覚えて下さい。

仮名加工情報。。

氏名や住所などの個人を特定できる情報を削除または置換し、他の情報と照合しない限り特定の個人を識別することができなくなったものです。他の情報と照合すればなまの個人情報に復元できるものなので、匿名加工情報にはない以下の規制があります。。。

1。対照表等の安全管理義務。。。

2。第三者への提供の原則禁止。。。

3。本人への到達行為の禁止。。。

4。利用目的の制限。。。

5。利用目的達成時の消去、努力義務

ミスインフォメーション。ご情報。。

悪い意図がなく拡散する偽りの情報のことです。見出しと中身が異なる、ミスリーディングを誘う内容などが該当します。

ディスインフォメーション。にせ情報。。

悪い意図があり意図的に拡散される偽りの情報のことです。虚偽の内容、なりすまし、見せ方を工夫、捏造などが該当します。

ペアレンタルコントロール。。

ペアレンタルは、親の、親としての、という意味の言葉で、コントロールは、制御する、管理する、操作する、というような意味です。子供が持つスマホやパソコンの利用方法を、保護者が管理する機能のことを指します。

分散ファイルシステム。ディストリビューテッドファイルシステム。DFS。。

データの格納、管理を簡素化するためのシステムのことです。ネットワーク上の複数のサーバの共有ストレージに格納されているデータファイルの一元管理を可能にし、ユーザやアプリケーションからのアクセスを容易にします。複数のサーバをクラスタ化することで、別々のマシンに分散するストレージリソースやデータファイルを多くのユーザが共有できるようにしています。

リバースプロキシサーバ。。

特定のサーバへの要求を中継する目的で設置されるサーバです。Webサイトなどにおける窓口として機能します。主な機能として、認証、暗号化、圧縮、負荷分散などが挙げられます。また、配信元のサーバのIPアドレスを明らかにする必要がなくなるため、攻撃者がディードス攻撃などを利用することが困難になり、セキュリティが強化されます。

ソブリンクラウド。。

経済安全保障の観点からデータやソフトウェアの主権を保持、コントロールできるクラウドサービスを指す言葉です。現時点では、統一されたソブリンクラウドの定義は存在せず、国や企業によってその形態が異なります。日本においては、データの主権を確保しつつ、クラウドコンピューティングの利便性を享受できるサービスや概念のことを指します。これは、データがどこに保存され、どのように利用されるかについてより厳密な制御を持ちたいというニーズから生まれたものです。

最高デジタル責任者。チーフディジタルオフィサー。しーでぃーおー。。

企業におけるデジタル化の推進を担当する役職のことを指します。CDOの主な役割は、企業のデジタルトランスフォーメーション、DXを導き、ITとビジネス戦略を一体化させることです。

リスキリング。。

新しい職業に就くために、あるいは、今の職業で必要とされるスキルの大幅な変化に適応するために、必要なスキルを獲得する、させることです。近年では、特にDX化のための新たなスキルの習得や、仕事の進め方が大幅に変わるであろう職業につくためのスキル習得を指すことが増えています。

Webクローリング。。

クローラーというプログラムがWeb上を巡って、WebページのリンクをたどりながらWebサイトを巡回し、Webページにある情報を保存・収集することです。くろーるは、はって行く、クロールで泳ぐ」という意味です。

スクレイピング。ウェブスクレイピング。。

ウェブサイトの情報を自動的に収集する手法のことです。これにより、大量のデータを効率的に収集することができます。具体的には、プログラムやスクリプトを使用してウェブページにアクセスし、そのページの内容を解析して必要な情報を抽出します。