Uma introdução sobre Cybersecurity e LGPD – Parte 1

Published on October 1, 2019

Waldemir Cambiucci

Technical Sales Manager | Director at Microsoft Technology Center São Paulo

Neste artigo, vamos falar sobre segurança no espaço digital, um tema cada vez mais importante para pessoas físicas e jurídicas e não é de hoje! O tema é muito vasto e muitas vezes complexo.

Assim, escolhi alguns tópicos principais para discussão, dividindo o texto em duas partes: no artigo de hoje, vamos focar sobre grandes conceitos e propriedades da segurança da informação, como integridade, privacidade, disponibilidade, proteção de dados, gestão de acesso, autenticação, autorização, gestão de aplicativos e dispositivos, além de ataques e riscos presentes no ambiente cibernético. Vamos finalizar a parte 1 com um mapa geral sobre a plataforma Microsoft e seus componentes para suportar segurança no ambiente de TI.

Na parte 2 dessa série, vamos falar de **LGPD – Lei Geral de Proteção de Dados**, que deve entrar em vigor em agosto de 2020. LGPD é nossa versão brasileira para ***GDPR – General Data Protection Regulation*** ou **Regulamento Geral sobre Proteção de Dados**, que entrou em vigor em maio de 2018 no direito europeu, protegendo dados de pessoas na União Europeia e Espaço Econômico Europeu em transações no cyber espaço. Vamos explorar alguns aspectos de GDPR e LGPD no Brasil e como as empresas devem

estar atentas ao tema antes da lei brasileira entrar em vigor. Até agosto de 2020, temos tempo de preparação e estudo, para suportar uma operação mais segura e em conformidade com a nova lei. Empresas que não estiverem em conformidade com a lei estarão em risco de penalidades previstas, além do próprio risco de segurança para suas marcas e negócios. Assim, não vale deixar essa jornada para depois do Carnaval! 😊 Vamos lá?

Introdução

Recentemente, vimos em reportagens de rádio e televisão que o Brasil sofre com o crescimento de golpes com a clonagem de contas do WhatsApp. Você deve ter ouvido falar desse golpe, que funciona assim:

1. uma vítima em potencial compartilha seu número de WhatsApp, por exemplo, através de anúncios de produtos em sites de comércio eletrônico, vendas de imóveis ou veículos, etc.;

2. o criminoso envia para a vítima uma mensagem se fazendo passar pela empresa onde o anúncio está publicado, pedindo uma atualização cadastral. O criminoso envia uma mensagem de 6 dígitos via SMS para a vítima e pede que esta repasse o código através do WhatsApp;

3. ao devolver o código para o criminoso, a vítima está clonando seu WhatsApp no aparelho do criminoso, que inicia imediatamente conversas com a lista de contatos da vítima, pedindo dinheiro ou outros benefícios;

Esse é um exemplo de golpe em meio cibernético com foco em pessoa física. O estrago gerado por esse golpe pode ser grande, seja financeiro ou como de imagem e reputação. Agora pense no impacto semelhante para empresas, startups, universidades ou órgãos de governo. De fato, estamos todos expostos 100% do tempo a ataques cibernéticos, que visam a captura de dados, informações, lista de contatos, acessos privilegiados, autorizações específicas, chaves de segurança, além de dinheiro. Falhas de infraestrutura, invasão de sistemas, dados sensíveis comprometidos ou compartilhados publicamente por hackers, infestação por vírus de computador, publicação de conversas por mensagens ou telefônicas, etc. são exemplos diversos de ataques presentes nos dias de hoje. Com um número cada vez maior de usuários móveis, aplicações digitais e redes de dados conectadas de forma global, as oportunidades para os chamados cyber criminosos tende a aumentar. Já faz tempo que falamos mesmo sobre uma nova modalidade de guerra no século XXI, a guerra cibernética, que ocorre no espaço virtual, com poder para derrubar pessoas, empresas ou até mesmo organizações e países.

Mas em sua essência, **ataques cibernéticos são executados por criminosos cibernéticos, que priorizam vítimas potenciais que possuem pouca ou nenhuma experiência, conhecimento ou proteção contra esses ataques.** Pessoas, empresas ou organizações que tratam com descasos ou despreparo e descuido sua proteção no meio digital são alvos mais fáceis e assim, alvos preferenciais. Esse é o caso de empresas de pequeno e médio porte, por exemplo, onde investimentos em cyber

segurança são pequenos ou inexistentes, realizando negócios e transações no meio online com elevada exposição.

Mas o que é Segurança da Informação?

Você vai encontrar inúmeras definições sobre segurança da informação, além de possui sua própria definição baseada em sua experiência e histórico profissional. Assim, vamos buscar um certo formalismo para ajudar no aprofundamento do tema.

Segundo a norma **ABNT NBR ISO/IEC 17799**, elaborada no Comitê Brasileiro de Computadores e Processamento de Dados (ABNT/CB-21), **a segurança da informação é a forma encontrada pelas organizações para proteger seus dados, através de regras e controles rígidos, estabelecidos, implementados e monitorados constantemente, a fim de assegurar a continuidade do negócio.**

Veja mais aqui: https://pt.wikipedia.org/wiki/ISO/IEC_17799

Essa definição é abrangente é bastante interessante, uma vez que envolve diversos pilares para garantir a continuidade do negócio. A figura a seguir ilustra esses diferentes componentes ou propriedades básicas da segurança da informação:

Figura 1 – propriedades básicas da segurança da informação.

No contexto de segurança da informação temos portanto:

Confidencialidade

· A confidencialidade garante que somente pessoas autorizadas tenham acesso ao dado ou informação envolvidos. Através da confidencialidade da informação, protegemos conteúdos

sensíveis da visualização, publicação ou acesso por pessoas não envolvidas diretamente com a informação, ou de externos a empresa não autorizados para esses acessos. Uma ferramenta para se garantir a confidencialidade dos dados, seja em trânsito (*data in transit*) ou armazenados (*data at rest*) é a criptografia.

Integridade

· A integridade dos dados garante que informações armazenadas em diferentes mídias ou repositórios permaneçam íntegros, resistentes a falhas, sem alterações ao longo do tempo. De igual modo, a integridade dos dados deve ser garantida tanto para dados em trânsito (*data in transit*), assim como para dados armazenados (*data at rest*). A integridade pode ser garantida através da manutenção de cópias de segurança ou backups, como citado na ISO 27040, por exemplo. Ferramentas que permitem garantir a integridade são backups de dados e assinaturas digitais, por exemplo.

Disponibilidade

· Tão importante quando integridade ou privacidade, garantir a disponibilidade da informação é pilar importante da segurança da informação. Permitir que a informação esteja acessível aos usuários a qualquer tempo esperado é objetivo deste princípio básico de segurança. Algumas ferramentas são comuns para se garantir disponibilidade, como como redundância de servidores, proteção contra falhas de energia, links e recursos backups, sistemas de recuperação de desastres (*D&R – Disaster Recovery*), entre outras.

Não-repúdio

· De modo simplificado, o não-repúdio pode ser definido como sendo "*suficiente evidência para persuadir uma autoridade legal (juiz, jurado ou árbitro) a respeito de sua origem, submissão, entrega e integridade, apesar da tentativa de negação pelo suposto responsável pelo envio*". Essa definição tem uma perspectiva mais jurídica e foi retirada do guia da *American Bar Association PKI Assessment Guidelines*, como referência. Em outras palavras, é a propriedade que garante sem dúvida que uma mensagem foi gerada e enviada por um determinado usuário, servindo como prova legal para qualquer situação de comprovação. É o caso de se garantir que certo correntista realizou um saque no *auto-atendimento* usando seu cartão de débito, a partir da submissão de sua senha pessoa de acesso, sem a possibilidade de negação do evento de saque, por exemplo.

Autenticidade

· Autenticidade consiste na certeza absoluta da veracidade ou originalidade de informação, garantindo assim sua identificação e a segurança da origem da informação. O nível de segurança desejado pode estar ligado a uma "política de segurança" que é seguida pela organização ou pessoa, para garantir que uma vez estabelecidos os princípios, aquele nível desejado seja

perseguido e mantido. Existem diversas ferramentas que podem garantir o princípio da autenticidade na segurança da informação, como biometrias, assinaturas digitais e certificados digitais. Um subproduto da autenticidade é o não-repúdio, por ser possível garantir a veracidade do conteúdo da informação e seu emissor.

Essas propriedades básicas da segurança fazem parte também do que chamamos de **Sistemas de Gestão de Segurança da Informação (SGSI)**, que visam a implementação, melhoria, revisão, funcionamento e análises no contexto da segurança digital.

O SGSI inclui estratégias, planos, políticas, medidas, controles e diversos instrumentos e ferramentas usados para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação. Uma ferramenta importante usada por um SGSI é a família de normas ISSO 27000, que tratam diferentes aspectos da segurança da informação.

Dentro da família de normas de segurança da ISO 27000 para segurança da informação destacamos:

- *ISO 27001 - Gerenciamento da Segurança da Informação*
- *ISO 27033-3 – Segurança em redes de computadores*
- *ISO 27033-4 – Comunicação segura entre rede e Gateways*
- *ISO 27033-5 – Comunicações segura para redes virtuais privadas (VPN)*
- *ISO 27033-6 – Segurança em Redes Sem Fio*
- *ISO 27036 – Segurança da Informação no relacionamento com fornecedores*
- *ISO 27039 – IDS (Intrusion Detection Systems) IPS (Intrusion Prevention Systems)*
- *ISO 27040 – Segurança de Armazenamento*

A norma ISO 27001 adota o modelo *PDCA (Plan-Do-Check-Act)* para apresentar a estrutura de um SGSI, o que facilita para as empresas o planejamento de uma estratégia de segurança e implantação de um sistema gestor. Veja na figura a seguir esse modelo:

Figura 2 – modelo PDCA adotado pela norma ISSO 27001.

Bastante coisa não é mesmo? 😊 Até aqui, vimos apenas alguns conceitos e propriedades importantes que criam o contexto de segurança da informação. Um tema igualmente crítico para esse estudo é a **SEGURANCA DE PERÍMETRO**, que veremos a seguir.

Segurança de perímetro

Pensar em **segurança da informação** significa proteger a informação em diferentes momentos de seu ciclo de vida, garantindo a integridade, a disponibilidade e a privacidade dos dados envolvidos. As fronteiras que irão cercar os domínios de informação em níveis de segurança aplicáveis definem os **perímetros de segurança**.

O conceito de **segurança de perímetro** vem do mundo físico e é um velho conhecido, mais especificamente do mundo militar. Todos nós usamos portas, janelas, muros, portões, etc., que fazem a proteção de nossas residências e empresas. Nesse caso, nosso perímetro de segurança é a linha que separa nossa casa da rua ou do espaço público do condomínio. Podemos adicionar elementos de proteção a esses perímetros de segurança com o uso de cadeados, correntes, travas, fechaduras, cachorros ou cercas eletrificadas, o que amplia o poder de proteção desses perímetros. Apenas pessoas autorizadas e com as chaves corretas de acesso podem circular dentro e fora dos perímetros de segurança definidos. Quanto maior for nossa proteção, maior a dificuldade para que uma pessoa transite livremente entre diferentes perímetros de segurança.

A história da humanidade é repleta de exemplos de perímetros de segurança, com seus exemplos maiores nos **castelos medievais**, que eram **verdadeiras fortalezas** para a proteção de cidadelas, recursos, tesouros ou pessoas importantes, não apenas com barreiras físicas como grandes muros intransponíveis, mas também através fossos, canais, pontes levadiças, proteções ativas e sistemas de batalha, como arqueiros, olheiros, falcões, caldeirões de óleo ferventes, catapultas e muitas espadas. Quem não se lembra de Minas Tirith, a capital fortificada do reino de Gondor, dos escritos da Terra Média 😉 Uma fortaleza gigantesca com uma enorme segurança de perímetro.

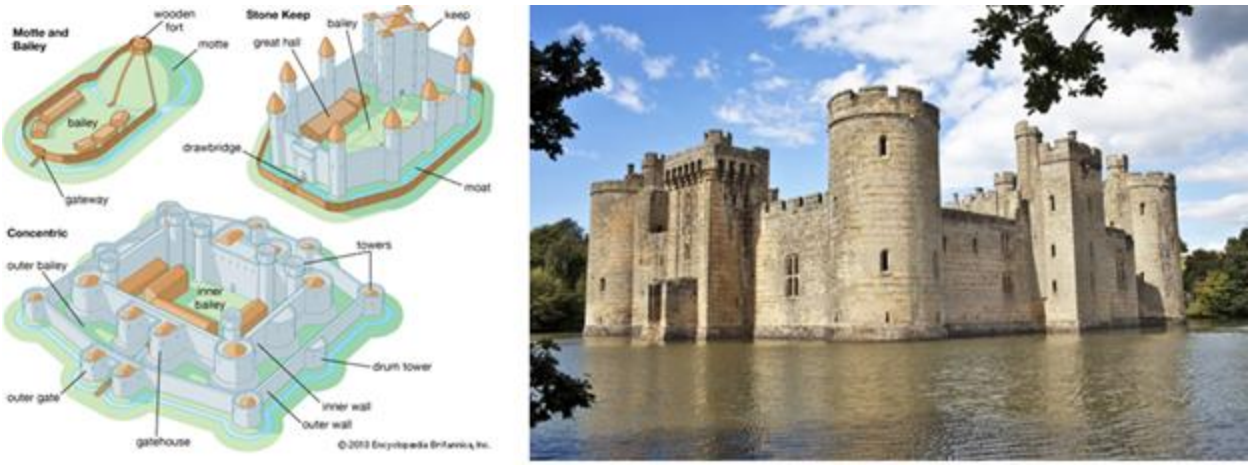

Figura 3 – fortalezas físicas para a proteção de dados reais; os primeiros perímetros de segurança eram feitos de pedra, madeira e aço forjado.

Assim, a **segurança de perímetro** envolve a implantação de tecnologias de rede para proteger rede corporativa contra invasões ou intrusos, por exemplo, a partir da internet ou via acessos desprotegidos.

A **segurança de perímetro** mudou ao longo do tempo, ampliando seus limites e adicionando novos participantes e fronteiras no meio digital. Por exemplo, para uma empresa, o perímetro de segurança ultrapassou as conexões locais de dentro da empresa com a internet, chegando aos notebooks dos usuários em casa, até os smartphones sempre conectados nas mãos de seus colaboradores ou fornecedores federados. Esses novos limites de segurança exigem novas medidas de proteção, até uma cultura de segurança mais ampla e adotada por pessoas de diferentes níveis, de profissionais a leigos e usuários.

Então o que é Cybersecurity?

A analogia com castelos medievais sob constantes ataques de tribos e exércitos inimigos é perfeita para sistemas de **cybersecurity**: qual é o tamanho de nossos muros? qual é a qualidade de nossos observadores? Como percebemos tentativas de invasão por intrusos? quais são as medidas que aplicamos para responder aos ataques em tempo real? Como percebemos intrusos tentando pular nossos muros digitais ou abrir nossas pontes? Temos ainda pontes abertas em nosso castelo?

Podemos definir **cybersecurity** como parte da **segurança da informação**, envolvendo uma superfície maior de exposição de dados e recursos pela internet, sob ataques de diferentes níveis de profundidade e complexidade.

De igual modo, você vai encontrar inúmeras definições sobre **cybersecurity** ou **segurança cibernética** na internet, cada uma com abordagens ou ênfases diferentes. Para simplificar, vou adotar a seguinte definição neste artigo:

· **Cybersecurity** ou **Segurança Cibernética** é uma parte importante da **Segurança da Informação**, combinando inúmeros métodos, técnicas e ferramentas que visam proteger de forma ativa, sistemas, informações e dados contra **ataques cibernéticos**.

Assim, **cybersecurity envolve técnicas, métodos e ferramentas que detectam e atuam em cenários de ataque no espaço online, protegendo a integridade, a disponibilidade e a privacidade de informações sensíveis de pessoas e empresas.**

Cybersecurity envolve diversos conceitos de segurança que constantemente se renovam, como:

- crimes cibernéticos
- guerra cibernética
- segurança de dispositivos e coisas em IOT
- regulações e conformidades com leis e normas
- segurança de infraestrutura
- privacidade de dados
- controle de acesso e identidade
- controle de senhas e certificados
- métodos de criptografia
- monitoração e orquestração de eventos
- detecção e reposta
- classificação de informações
- gerenciamento de aplicações
- gerenciamento de dispositivos
- vírus e infestações digitais
- ataques digitais em massa

A lista acima é parcial e pode crescer com o tempo. Podemos afirmar que segurança da informação envolve tecnologias que estão em constante evolução. Dentro do escopo de **cybersecurity**, alguns temas merecem especial destaque, como veremos a seguir.

EDR - Endpoint Detection and Response

Endpoint Detection and Response, ou EDR, é uma tecnologia que oferece monitoramento e resposta contínuos contra ameaças avançadas em segurança cibernética. O EDR é um subconjunto da ***segurança de endpoint***, que lida com a proteção de redes e dados corporativos quando os usuários acessam a rede remotamente a partir de notebooks, desktops, smartphones ou outros dispositivos móveis externos, fora do perímetro físico das empresas.

A ***segurança de endpoint*** tem por objetivo garantir a **segurança geral do dispositivo na ponta**, assim como a rede corporativa envolvida contra vulnerabilidades, ataques de hackers ou outras ameaças cibernéticas.

Já o ***Endpoint Detection and Response (EDR)*** se concentra especificamente em apoiar a identificação, investigação e resolução de ameaças avançadas e grandes ataques cibernéticos que podem comprometer diversos endpoint ao mesmo tempo. EDR é uma ferramenta importante para times de segurança ativos na batalha contra cyber criminosos.

A adoção de soluções EDR permite um maior controle contra incidentes, quando comparamos com métodos tradicionais, como os antivírus, garantindo que comportamentos anômalos ou ações maliciosas sejam identificados rapidamente, permitindo o tratamento de brechas de segurança e respostas mais rápidas.

Network Intrusion Detection/Intrusion Prevention Systems (IDS/IPS)

Podemos dizer que **EDR** é uma ferramenta moderna, uma evolução dos chamados ISD/IPS, que aplicavam técnicas similares para armazenar, correlacionar e analisar ocorrências de segurança, como tentativas de acesso, envio de mensagens, etc. A diferença é que EDR atualmente tem um foco maior sobre os *endpoint* envolvidos e seus diferentes **metadados**, permitindo que diferentes tipos de correlações em alertas de segurança e diferentes técnicas de detecção sejam aplicadas, olhando em maior profundidade um conjunto maior de logs e registros armazenados.

Security Information Event Managers (SIEM)

Chamamos sistemas **SIEM - Security Information and Event Management** de ferramentas de software que combinam o gerenciamento de segurança da informação com o gerenciamento de eventos de segurança no meio digital. Sistemas SIEM oferecem análise em

tempo real sobre alertas de segurança gerados por aplicações, sistemas e infraestrutura de redes e computadores.

Sistemas SIEM já são velhos conhecidos de times de segurança em ambiente corporativo, pelas inúmeras facilidades que oferecem para equipes no processo de análise e tratamento de alertas. Existem diversas vantagens e capacidades oferecidas por sistemas SIEM, como:

· Detecção de anomalias que podem ajudar a detectar códigos Zero-Days ou assinaturas polimórficas em ataques de vírus e outros tipos de malware;

· Análise, normalização e classificação de logs que podem ocorrer automaticamente, independentemente do tipo de dispositivo na rede;

· Visualização de eventos de segurança e falhas, agilizando a detecção de padrões de comportamento e ataques em tempo real;

· Anomalias em protocolos podem indicar uma configuração incorreta ou um problema de segurança, que são facilmente identificados com SIEM;

· SIEM pode detectar comunicações ocultas e mal-intencionadas em canais criptografados pela rede;

· Finalmente, a chamada guerra cibernética pode ser detectada através de SIEMs com precisão, descobrindo atacantes e vítimas em tempo de resposta;

Essas diferentes capacidades permitem uma rápida atuação pelos times de segurança, velocidade cada vez mais importante com a elevada exposição global via internet.

Security Orchestration Automation and Response (SOAR)

Como vimos, SIEM já faz parte da estratégia de segurança de muitas empresas há anos. A novidade é o SOAR, sigla para **Security Orchestration Automation and Response**.

O termo SOAR foi criado pelo Gartner, cobrindo tecnologias de cybersecurity que aplicam técnicas de artificial Intelligence e máquinas de aprendizado. Veja um belo texto sobre SOAR nesse link: https://www.alienvault.com/blogs/security-essentials/security-orchestration-automation-and-response-soar-the-pinnacle-for-cognitive-cybersecurity

Com o uso amplo de técnicas de inteligência artificial em diferentes cenários de indústria, não seria difícil esperar o uso de **Machine Learning** (ou máquinas de aprendizado) também na identificação de comportamentos e padrões de ataque em cenários de segurança da informação. É o que estamos vendo cada vez mais com o uso de algoritmos para a detecção de padrões em

eventos de segurança e alertas gerados por redes de computadores. Milhões de linhas de log são usados para alimentar bases de treinamento de algoritmos de **machine learning**, com o objetivo de reconhecer padrões de ataques e gerar alertas de forma antecipada, nos primeiros indícios de novas ocorrências no futuro.

Esse é o caso para a tecnologia SOAR, capaz de agregar informações diversas de fontes externas, como dashboards de segurança em infraestrutura, logs de e-mails, logs de *requests* HTTP, mensageria de SQL *requests*, etc, ampliando o quadro de segurança dentro e fora da organização. Esse mapa maior contempla não apenas os alertas de segurança observados por sistemas SIEM, mas também a orquestração de investigações configuráveis, que times de segurança podem aplicar em seus domínios de análise.

Assim, o time de segurança pode adotar *playbooks* de investigação sobre o SOAR e otimizar seus caminhos de investigação, sobre bases históricas de alertas de segurança, reduzindo o tempo gasto com alertas e automatizando ações ou medidas de resposta, aumentando a eficiência dos times de segurança.

Cloud Access Security Brokers (CASB)

Outro importante conceito em cybersecurity é o CASB. Em português, um **broker de segurança de acesso à nuvem** é um software local ou baseado na nuvem que fica entre os usuários de serviços e aplicativos em nuvem, monitorando todas as atividades realizadas, aplicando políticas de segurança durante sua operação.

Um CASB pode oferecer uma variedade de serviços, incluindo o monitoramento das atividades do usuário, alerta para administradores e times de segurança sobre ações perigosas ou de risco, aplicando conformidades políticas de segurança adotadas e prevenindo ataques ou propagação de malwares. O CASB oferece essa proteção através de 4 pilares importantes: visibilidade, conformidade, segurança de dados e proteção contra ameaças, alguns desses que vimos anteriormente nesse artigo.

Security Operations Centre (SOC)

Centros Operacionais de Segurança é um termo genérico que descreve boa parte ou totalidade de uma plataforma de serviços de detecção e reação a incidentes de segurança. Um SOC pode executar 6 grandes operações, sendo:

- Identificação de eventos de segurança;
- Coleta de dados;
- Armazenamento de eventos;
- Análise;

- Reação;
- Observação

Um SOC pode ser interno e dedicado a uma única empresa, ou mesmo ser terceirizado e suportar inúmeras empresas, quando chamamos de **Virtual SCO** ou **VSOC**. Serviços gerenciados de segurança são bastante promissores e podem ser um elemento crítico na estratégia de segurança de várias empresas para os próximos anos, com uma maior adoção de uma cultura de segurança no campo.

DevSecOps

DevSecOps significa pensar na segurança da aplicação e na infraestrutura de segurança envolvidos no projeto desde seu início, dentro de uma abordagem **DevOps** de desenvolvimento ágil. Esse envolvimento de profissionais de segurança durante os primeiros estágios no desenvolvimento do software também enfatiza a adoção de uma **codificação segura** ou **S-SDLC | Secure Software Development Life Cycle**, antecipando soluções necessárias durante o projeto.

O conceito de **DevSecOps** é mais um importante aliado na construção de uma estratégia de segurança em toda organização, garantindo que o software produzido seja realizado com segurança desde sua concepção.

No site a seguir encontramos o manifesto **DevSecOps**, que ilustra muito bem esse objetivo de SOFTWARE SAFER SOONER. https://www.devsecops.org/

PIM (Privileged Identity Management)

Um recurso também importante em segurança é a necessidade de gerenciar, controlar e monitorar acessos a recursos críticos ou sensíveis da organização. Cenários assim exigem uma monitoração ativa e especial, que permite a organização minimizar o número de pessoas que possuem acesso a informações seguras ou recursos escolhidos, reduzindo a exposição desses recursos a um número maior de acessos ou autorizações, com potencial impacto para visualizações indesejáveis.

Software Asset Management (SAM)

Finalmente, o **Gerenciamento de Ativos de Software (SAM)** também pode ser colocado na lista de temas ligados a segurança da informação e cybersecurity, uma vez que envolve conformidades legais e gestão de licenças de software ativos operando sobre os dados de nossa organização. SAM oferece um conjunto de práticas de TI que reúne pessoas, processos e tecnologia para controlar e otimizar o uso de software em uma organização. De igual modo, SAM pode ajudar no controle de custos e gestão de riscos de negócios, otimizando investimentos

em licenciamento de software e garantindo a legalidade de licenças e estações ativas sobre assets da empresa. Uma constante revisão do catálogo de software

Vimos assim uma introdução sobre **segurança da informação** e **cybersecurity**. São inúmeras disciplinas e conceitos, que definem uma jornada igualmente longa e vibrante. Temas como testes de intrusão (*PenTest*), ataques cibernéticos, ferramentas e métodos de engenharia social, técnicas de força bruta, etc. completariam esse vasto universo que está em constante mutação.

A seguir, vamos falar sobre alguns dos principais componentes de segurança em plataforma Microsoft, que suportam uma estratégia de segurança da informação. Todos comigo? 😉

Um mapa de cybersecurity em plataforma Microsoft

Aqui, vou aproveitar um mapa de plataforma Microsoft que foi trabalhado pelo amigo Maiko Oliveira, especialista em segurança da Microsoft no Brasil. Valeu Maiko!

O desenho é bastante interessante, uma vez que agrupa os principais componentes de plataforma com impacto direto para a segurança da informação.

Veja que cada um dos pilares de segurança que discutimos ao longo do artigo encontra uma ferramenta ou componente em plataforma Microsoft, como a seguir:

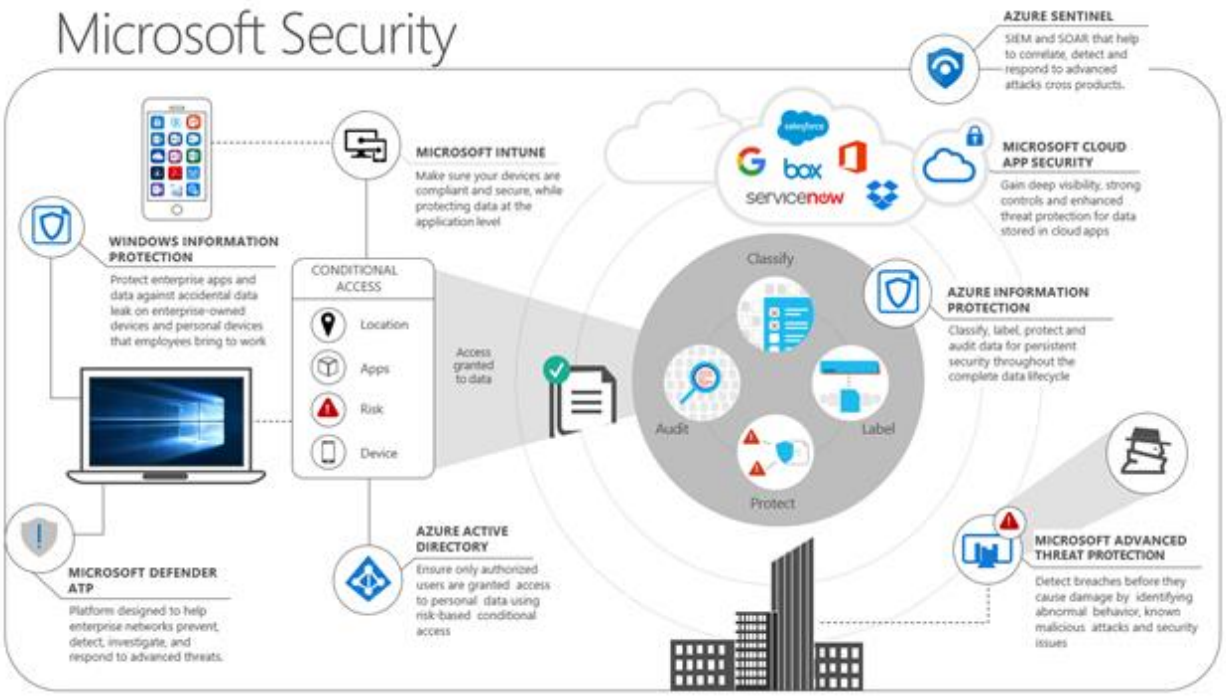

Figura 4 – alguns componentes de segurança em plataforma Microsoft.

Veja que no centro temos a empresa, com seus dados e informações críticas que precisamos proteger. De igual modo, usuários acessam informações diversas, usando dispositivos, aplicações ou credenciais e identidades, que precisamos garantir quanto a autenticidade e autorização no momento do acesso.

Diferentes tipos de dados podem ser classificados quanto ao impacto e criticidade, determinando assim suas exigências em relação a proteção ou impacto em caso de vazamento. Finalmente, em ataques virtuais em andamento, precisamos garantir que equipes de segurança tenham ferramentas adequadas para monitorar, detectar e responder de forma ágil e em tempo de resposta, assim que esses ataques são percebidos.

Para cada momento dessa história de segurança podemos destacar uma ferramenta com aplicação específica, com destaque para:

WINDOWS INFORMATION PROTECTION

· Proteja aplicativos e dados corporativos contra vazamento acidental de dados em dispositivos de propriedade da empresa e dispositivos pessoais que os funcionários trazem para o trabalho.

MICROSOFT DEFENDER ATP

· Plataforma projetada para ajudar redes corporativas a prevenir, detectar, investigar e responder a ameaças avançadas.

MICROSOFT INTUNE

· Verifique se seus dispositivos são compatíveis e seguros, protegendo os dados no nível do aplicativo.

AZURE ACTIVE DIRECTORY

· Garantir que apenas usuários autorizados tenham acesso a dados pessoais usando acesso condicional com base em risco

MICROSOFT ADVANCED THREAT PROTECTION

· Detecte violações antes que causem danos, identificando comportamento anormal, ataques maliciosos conhecidos e problemas de segurança.

AZURE INFORMATION PROTECTION

· Classifique, rotule, proteja e audite dados para segurança persistente durante todo o ciclo de vida dos dados.

MICROSOFT CLOUD APP SECURITY

· Obtenha visibilidade profunda, controles fortes e proteção aprimorada contra ameaças para dados armazenados em aplicativos em nuvem.

AZURE SENTINEL

· SIEM e SOAR que ajudam a correlacionar, detectar e responder a ataques avançados entre produtos.

Na parte 2 dessa série, vamos explorar em detalhes alguns desses componentes, enquanto falamos sobre arquiteturas de referência para segurança em plataforma Microsoft. Fique ligado.

Considerações

No início do artigo ilustrei o golpe de sequestro de conta de WhatsApp. Assim, segue aqui algumas dicas de como evitar esse golpe:

1. ative a verificação de identidade como duplo fator no WhatsApp, através do menu CONFIGURAÇÕES / CONTA / CONFIRMAÇÃO EM DUAS ETAPAS. Você poderá cadastrar um PIN único e uma conta de EMAIL para verificações regulares de sua identidade;

2. Nunca repasse códigos de SMS para terceiros: não é comum o uso de SMS por empresas de comércio eletrônico ou mesmo bancos com clientes;

3. Nunca realize transações financeiras sem antes checar com certeza a identidade da pessoa com quem estiver falando;

Pronto, você está um pouco mais seguro, pelo menos em relação a seu WhatsApp. :)

Vale destacar que cobrimos aqui apenas alguns componentes e temas de segurança da informação, fazendo uma breve introdução sobre o assunto.

A complexidade em torno de segurança é devido a sua abrangência e diversidade de conceitos e cenários envolvidos com a proteção de informações. Existem inúmeros temas que merecem ainda especial atenção, como criptografia, tokens de segurança, certificados digitais, duplo fator de autenticação (MFA – MULTI FACTOR AUTHENTICATION), mecanismos de atualização de software, provedores de identidades, SAML, OAUTH, HTTP/HTTPS, TLS, protocolos criptográficos, DEVSECOPS, SSO – SINGLE SIGN-ON, CONDITIONAL ACCESS, entre outros. Estes temas ficarão para artigos futuros!

No próximo artigo, vamos continuar falando de segurança, focando aspectos da nova lei de proteção de dados no Brazil, a LGPD e seu impacto para empresas em operação no cyber espaço. Vamos também olhar uma arquitetura de referência para **cybersecurity** e completar a discussão com alguns roadmaps de certificações e provas em segurança, para você continuar seus estudos e avançar em seu TECH INTENSITY.

Por enquanto é só! Até a próxima!

Waldemir.

Referências

Microsoft cloud for enterprise architects series

- https://docs.microsoft.com/en-us/office365/enterprise/microsoft-cloud-it-architecture-resources#cloudarch

Proteger os dados empresariais usando a Proteção de Informações do Windows (WIP)

- https://docs.microsoft.com/pt-br/windows/security/information-protection/windows-information-protection/protect-enterprise-data-using-wip

Proteção avançada contra ameaças do Microsoft defender

- https://docs.microsoft.com/pt-br/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-advanced-threat-protection

What's new in Windows Defender ATP

- https://www.microsoft.com/security/blog/2018/11/15/whats-new-in-windows-defender-atp/

What is Microsoft Intune?

- https://docs.microsoft.com/pt-br/intune/what-is-intune

Gerenciamento de Ativos de Software

- https://www.microsoft.com/pt-br/sam/basics.aspx?CollectionId=9d33c0b2-7c54-4274-8b1c-d1dec3b8548d

What is Azure Active Directory?

- https://docs.microsoft.com/pt-br/azure/active-directory/fundamentals/active-directory-whatis

O que é a Proteção Avançada contra Ameaças do Azure?

- • https://docs.microsoft.com/pt-br/azure-advanced-threat-protection/what-is-atp

O que é o Azure Information Protection?

- https://docs.microsoft.com/pt-br/azure/information-protection/what-is-information-protection

Visão geral do Microsoft Cloud App Security

- https://docs.microsoft.com/pt-br/cloud-app-security/what-is-cloud-app-security

Azure Sentinel

- https://azure.microsoft.com/pt-br/pricing/details/azure-sentinel/