Tendências de Cybersecurity

Cybersecurity tem se mostrado ser uma corrida de gato e rato.

Em um mundo cada dia mais digital, nada mais natural do que se dar a atenção proporcional para Cybersecurity.

Mas ainda assim, creio que se faz necessário expor e explicar os principais conceitos

desse tópico para o grande público.

E para tanto, creio que esse webinar do Gartner vem para ajudar muita gente:

https://webinar.gartner.com/591158/agenda/session/1321558?login=ML

Nele é apresentada uma visão interessante dos grandes conceitos que estão despontando como tendências de mercado.

Para muitos os artigos podem ser básicos demais, mas para boa parte do público ajuda a ter uma visão ao menos panorâmica sobre cada tema tratado.

Em um mundo cada vez mais digitalizado e interconectado, a cibersegurança emerge como um pilar central para a proteção de ativos digitais e a manutenção da confiança no espaço cibernético.

O webinar do Gartner

O relatório da Gartner para 2023-2024 sublinha uma série de previsões cruciais que moldarão o cenário da cibersegurança nos próximos anos.

Entre elas, destaca-se a expansão e aprimoramento regulatório da privacidade, que cobrirá a maioria dos dados dos consumidores até 2024, mas menos de 10% das organizações conseguirão utilizar a privacidade como uma vantagem competitiva.

Este panorama sugere uma crescente complexidade no manejo da privacidade e proteção de dados, exigindo das organizações uma postura proativa e inovadora.

Outra previsão significativa aponta que até 2025, 50% dos líderes de cibersegurança terão tentado, sem sucesso, usar a quantificação de riscos cibernéticos para influenciar a tomada de decisões nas empresas.

Isso reflete os desafios associados à tradução de dados de segurança em insights acionáveis que possam efetivamente orientar as estratégias empresariais.

A adoção de práticas centradas no ser humano até 2027 é outro ponto crucial, indicando um deslocamento das práticas de segurança de uma visão centrada na tecnologia para uma mais focada no humano, com o objetivo de minimizar atritos e maximizar a adoção de controles de segurança.

Este é um reflexo da necessidade de equilibrar as medidas de segurança com a usabilidade e a experiência do usuário.

O aspecto regulatório sobre o tema de cybersecurity

Uma outra matéria recente abordou o aspecto da GPDR da Europa de forma associada ao tema de Cybersecurity, sob a perspectiva de privacidade de dados.

Tenho dúvidas se as regulações americanas (pelo visto lá existe muita coisa específica por cada estado) abordam “apenas” esse tema de dados ou se exploram outros aspectos.

Creio que já estamos no caminho por aqui a partir da LGPD, mas se forem aspectos diferentes, possivelmente em algum futuro próximo teremos outras regulações de segurança a serem importadas para cá.

O tamanho potencial do buraco negro das perdas por issues de cyber.

Alguns artigos estão falando que as perdas por temas de Cybersecurity serão algo na casa de USD 10,5 trilhões ao ano por volta de 2025 (que está logo ai).

Em um primeiro impulso eu até pensei que poderia ser uma hype na linha do Metaverso, mas na mesma matéria colocam que essa cifra seria um aumento na ordem de 300% versus os números de 2015, o que me parece ser, ao menos em grandes números, algo plausível, pois (infelizmente) nessa corrida de gatos e ratos, os ratos têm sido cada vez mais espertos.

E eu não cheguei a ler nada a respeito ainda, mas acho que seria natural esperar que os avanços tecnológicos atuais deverão trazer novas e melhores ferramentas para ambos os lados.

O que será que pode representar o poder da AI, Cloud, conectividade 6G ou até mesmo Quantum Computing sendo usados para o crime?

Acho que é legítimo pensar que podem no mínimo representar todo um novo mundo de oportunidades a serem exploradas, por ambos os lados, seja para atacar, seja para defender.

O mercado de trabalho em Cybersecurity

Acho que vale analisar sob a perspectiva do mercado de trabalho. Muito se falar sobre inúmeras oportunidades em Data Analytics e agora mais fortemente em AI, e com toda a razão, afinal são temas com ainda muito espaço para crescer.

Mas uma área que acaba muitas vezes não recebendo o mesmo destaque (será que é por ser menos “fancy”?) é justamente Cybersecurity. E considerando o exposto no artigo, tem tudo para ser (e provavelmente já é) uma área cheia de oportunidades.

Tenho a impressão (embora sem base em números, é só percepção mesmo) que os canais e mecanismos de formação são menores (ou divulgados em menor escala) que os outros temas com mais hype em IT.

Para quem busca um espaço em IT, vale avaliar essa área, muito embora, fica igualmente minha percepção de que aqui a régua é mais alta e é preciso já ter algum nível mínimo de conhecimento técnico para buscar então esse tipo de especialização.

CIO Codex Framework – Cybersecurity

Cybersecurity é um tema de vital importância na camada New Tech do CIO Codex Agenda Framework, refletindo uma necessidade crítica no cenário digital contemporâneo.

Este tema aborda as estratégias, tecnologias e práticas destinadas a proteger sistemas, redes e programas de ataques digitais.

O conteúdo complementar explora a complexidade crescente do cenário de ameaças cibernéticas e como as organizações podem desenvolver uma abordagem robusta para proteger suas informações e infraestruturas críticas contra uma variedade de riscos.

A introdução ao tema Cybersecurity enfatiza a importância de uma abordagem abrangente e multidimensional para a segurança cibernética.

Esta abordagem não se limita apenas à tecnologia, mas engloba processos, políticas, formação de equipes e cultura organizacional.

É discutido como a segurança cibernética é fundamental não apenas para a proteção de dados e sistemas, mas também para a manutenção da confiança dos clientes, a proteção da reputação da marca e a conformidade com regulamentos e padrões.

Este conteúdo explora os diversos aspectos da Cybersecurity, incluindo a identificação

de riscos, a proteção de ativos de TI, a detecção de ameaças, a resposta a incidentes e a recuperação de ataques.

São abordadas as tecnologias e práticas mais recentes em segurança cibernética, como criptografia avançada, autenticação multifatorial, inteligência artificial e aprendizado de máquina para a detecção de ameaças, bem como a importância de estratégias proativas como a análise de riscos e a realização de testes de penetração.

Além disso, são examinados os desafios em manter um ambiente de TI seguro, como a rápida evolução das ameaças cibernéticas, a complexidade crescente dos sistemas de TI e a escassez de profissionais qualificados em segurança cibernética.

São discutidas estratégias para construir e manter uma equipe de segurança cibernética eficaz, a necessidade de treinamento contínuo e conscientização em todos os níveis da organização, e a importância de colaborações e compartilhamento de informações sobre ameaças dentro da comunidade de segurança cibernética.

Por fim, o conteúdo destaca como medir a eficácia das iniciativas de Cybersecurity, incluindo a avaliação da postura de segurança, o monitoramento de indicadores-chave de desempenho e a realização de auditorias regulares.

É enfatizada a necessidade de uma abordagem dinâmica e adaptativa à segurança cibernética, que possa responder às mudanças no ambiente de ameaças e às novas exigências regulatórias.

Visão prática

Os componentes de cybersecurity extrapolam em muito os aspectos tecnológicos e devem ser considerados dentro de um Programa de Cybersecurity.

A criação de um programa de cibersegurança robusto e eficaz requer a definição e implementação de várias estruturas e processos chave.

Os componentes principais de um programa de cibersegurança incluem o mandato executivo, modelo de referência, estruturas de governança, plano estratégico anual e processos de segurança.

Cada um desses componentes é essencial para a criação de um programa de cibersegurança que não apenas protege a organização contra ameaças imediatas, mas também contribui para sua estabilidade e crescimento a longo prazo.

1) – Enterprise security charter: Executive mandate

O mandato executivo, ou carta de segurança empresarial, estabelece a autoridade e o compromisso da liderança sênior com a segurança cibernética.

Este documento é crucial porque define o tom e o suporte para todas as iniciativas de segurança dentro da empresa.

Ele deve esclarecer as expectativas da liderança, os recursos alocados e as responsabilidades de segurança em todos os níveis organizacionais.

A presença de um mandato claro e forte do executivo é um indicador de que a segurança é uma prioridade estratégica, não apenas uma necessidade operacional ou uma resposta a regulamentações.

2) – Terms of reference: Reference mode

Os termos de referência descrevem o escopo, os objetivos e os padrões específicos que orientam o programa de cibersegurança.

Eles servem como um modelo de referência que define as práticas, os procedimentos e os benchmarks contra os quais o programa será desenvolvido e avaliado.

Este componente é fundamental para assegurar que o programa de segurança esteja alinhado com as melhores práticas da indústria e com as necessidades específicas da empresa.

O modelo de referência ajuda a garantir consistência e qualidade nas iniciativas de segurança, facilitando também a comunicação e o entendimento claros dos objetivos de segurança em toda a organização.

3) – Governance structures: Accountability

As estruturas de governança referem-se ao conjunto de políticas, procedimentos e responsabilidades estabelecidos para gerir e monitorar o programa de cibersegurança da organização.

A responsabilidade é fundamental neste contexto, pois define quem é responsável por cada aspecto da segurança, desde a tomada de decisões até a implementação e a supervisão das políticas de segurança.

Uma governança eficaz assegura que haja clareza de responsabilidades, transparência nas decisões e um mecanismo para a prestação de contas.

Isso não só aumenta a eficácia do programa de segurança, mas também reforça a confiança de todas as partes interessadas na capacidade da organização de proteger

seus ativos.

4) – Annual strategy plan: Roadmap

O plano estratégico anual, ou roteiro, é o plano detalhado que define como as metas de segurança serão alcançadas durante o ano.

Este plano deve incluir objetivos específicos, iniciativas prioritárias, recursos necessários e prazos para implementação.

O roteiro serve como um guia para a equipe de segurança, garantindo que todos os esforços estejam alinhados com as metas estratégicas da empresa e com as expectativas dos stakeholders.

Ele também facilita a avaliação periódica do progresso e os eventuais ajustes das estratégias conforme necessário para responder a novos desafios e oportunidades.

5) – Security processes: Execution

Finalmente, os processos de segurança referem-se à execução prática das estratégias e políticas de segurança.

Este componente abrange a implementação de controles técnicos, a condução de auditorias e testes de penetração, a gestão de incidentes e a formação contínua dos funcionários.

A eficácia dos processos de segurança é crucial para a capacidade da organização de detectar, prevenir e responder a ameaças cibernéticas.

A execução rigorosa e eficiente dos processos de segurança garante que as medidas de proteção estejam sempre atualizadas e sejam eficazes, minimizando assim os riscos para a empresa e maximizando a confiança dos clientes e parceiros.

Evolução Cronológica

A trajetória da segurança cibernética é marcada por desenvolvimentos significativos que refletem as mudanças nas demandas tecnológicas e empresariais.

A seguir é apresentada uma visão detalhada da evolução cronológica da segurança cibernética, desde suas origens conceituais até as inovações mais recentes, ilustrando como essa disciplina revolucionou a infraestrutura de TI nas organizações.

A segurança cibernética continua a evoluir, respondendo tanto às oportunidades tecnológicas quanto aos desafios operacionais.

À medida que novas tecnologias emergem e as ameaças evoluem, as estratégias de segurança devem permanecer ágeis e adaptativas.

A capacidade de uma organização de se adaptar eficientemente será crucial para manter a competitividade e a segurança em um ambiente empresarial que é, por natureza, volátil e em constante evolução.

1) – As Origens da Segurança Cibernética (Anos 1970 – 1990)

- Primeiros Conceitos de Segurança: Nos anos 1970, com o surgimento dos primeiros sistemas de computação em rede, a necessidade de segurança começou a ser reconhecida. O desenvolvimento do modelo de segurança Bell-LaPadula, que se focava na confidencialidade dos dados, marcou um dos primeiros esforços teóricos significativos na área.
- Primeiros Vírus e Ataques: Nos anos 1980, a criação de vírus de computador como o "Elk Cloner" e o "Brain" destacou a necessidade crescente de segurança. As empresas começaram a desenvolver software antivírus e firewalls básicos para proteger seus sistemas.

2) – A Era da Internet e a Expansão da Ameaça (Anos 1990 – 2000)

- Explosão da Internet: Com a popularização da Internet nos anos 1990, as ameaças cibernéticas aumentaram exponencialmente. Ataques como o worm Morris em 1988 demonstraram a vulnerabilidade dos sistemas interconectados.
- Desenvolvimento de Protocolos de Segurança: Nesta década, surgiram os primeiros padrões de segurança, como o SSL (Secure Sockets Layer), para proteger a comunicação na web. As empresas começaram a investir em firewalls mais avançados, sistemas de detecção de intrusões (IDS) e soluções de criptografia para proteger suas redes.
- Regulamentações e Conformidade: A década de 1990 também viu o início da regulamentação de segurança, com leis como a Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA) nos EUA, que exigia a proteção de informações de saúde.

3) – A Era dos Ataques Sofisticados (2000 – 2010)

- Evolução das Ameaças: Nos anos 2000, os ataques cibernéticos tornaram-se mais sofisticados e direcionados. Adoção de técnicas como phishing, spear-phishing e ataques de negação de serviço (DDoS) aumentaram significativamente.
- Segurança em Camadas: A abordagem de segurança em camadas começou a ser adotada, combinando firewalls, sistemas de detecção e prevenção de intrusões (IDP/IPS), antivírus e criptografia. Surgiram também as primeiras soluções de gerenciamento de informações e eventos de segurança (SIEM) para monitorar e analisar logs de segurança.
- Cybercrime Organizado: O cybercrime passou a ser mais organizado, com grupos hackers profissionais focando em roubo de dados e extorsão. Casos como o ataque ao TJX em 2007, que resultou no roubo de dados de milhões de cartões de crédito, destacaram a gravidade da ameaça.

4) – A Era da Defesa Proativa e Automação (2010 – Presente)

- Avanços em Defesa Cibernética: Nos anos 2010, a segurança cibernética começou a focar em defesa proativa e resposta a incidentes. Tecnologias como inteligência artificial e aprendizado de máquina começaram a ser utilizadas para detectar comportamentos anômalos e ameaças em tempo real.
- Zero Trust e Segurança Baseada em Identidade: O modelo de segurança Zero Trust, que pressupõe que nenhuma rede, interna ou externa, é segura por padrão, ganhou popularidade. A segurança baseada em identidade e a gestão de acesso privilegiado (PAM) tornaram-se essenciais para proteger dados sensíveis.
- Regulamentação Rigorosa: A introdução de regulamentações rigorosas, como o Regulamento Geral sobre a Proteção de Dados (GDPR) na Europa e a Lei de Privacidade do Consumidor da Califórnia (CCPA), destacou a importância da proteção de dados e privacidade.
- Cyber Threat Intelligence e Automação: A utilização de inteligência contra ameaças (CTI) para antecipar ataques e a automação de respostas a

incidentes através de plataformas SOAR (Security Orchestration, Automation, and Response) tornou-se uma prática comum para melhorar a eficiência e eficácia da segurança cibernética.

5) – O Futuro da Segurança Cibernética

- Segurança em Ambientes Multicloud e Edge Computing: À medida que as empresas adotam ambientes multicloud e edge computing, novas abordagens de segurança serão necessárias para proteger dados distribuídos e descentralizados.
- IA e Machine Learning na Segurança: A integração de IA e machine learning continuará a crescer, permitindo a detecção e resposta a ameaças em tempo real com maior precisão. Essas tecnologias ajudarão a identificar padrões de ataque antes que causem danos significativos.
- Segurança de IoT: Com a proliferação de dispositivos IoT, a segurança desses dispositivos será crítica. A criação de padrões e protocolos específicos para a segurança de IoT será essencial para mitigar riscos.
- Cibersegurança e Resiliência Organizacional: A resiliência cibernética, que envolve a capacidade de uma organização se recuperar rapidamente de ataques cibernéticos, será um foco crucial. Planos de resposta a incidentes, backup e recuperação de dados e treinamentos contínuos serão fundamentais.
- Quantum Computing e Criptografia: A evolução da computação quântica apresentará novos desafios para a criptografia. Pesquisas em criptografia resistente a quântica serão vitais para proteger dados em um futuro em que os computadores quânticos possam quebrar algoritmos criptográficos tradicionais.

Em suma, a evolução da segurança cibernética tem sido uma jornada de transformação contínua, marcada por avanços tecnológicos significativos e desafios complexos.

À medida que essas tecnologias continuam a se desenvolver, elas prometem transformar ainda mais a forma como as organizações operam, oferecendo novos insights e oportunidades para inovação e proteção.

Conceitos e Características

A cibersegurança, um campo crítico da tecnologia, evoluiu para se tornar uma complexa malha de práticas, soluções e regulamentos destinados a proteger sistemas, redes e programas de ataques digitais.

Em sua essência, a cibersegurança é a aplicação de tecnologias, processos e controles projetados para proteger sistemas, redes e dados de ciberataques.

Efetiva cibersegurança reduz o risco de ataques cibernéticos e protege contra a exploração não autorizada de sistemas, redes e tecnologias.

Alguns conceitos e características se destacam nesse tema, como os apontados a seguir:

Confidencialidade, Integridade e Disponibilidade (CID)

A CID é um modelo que guia as políticas de segurança da informação para proteger a privacidade dos dados, prevenir erros e inacessibilidade.

Criptografia

Um método essencial de proteger informações, transformando-as em um código para prevenir acessos não autorizados.

Segurança de Rede

Inclui medidas para proteger a infraestrutura de TI contra intrusões, como firewalls, anti-malware, e sistemas de detecção de intrusão.

Segurança de Aplicações

Foca no manter o software e os dispositivos livres de ameaças. Um aplicativo comprometido poderia prover acesso a dados projetados para serem protegidos.

Recuperação de Desastres/Business Continuity Planning

Prepara a organização para responder a incidentes de cibersegurança e retomar as operações normais o mais rápido possível.

Características da Cibersegurança:

Adaptação Contínua

O campo exige uma adaptação e atualização contínua em resposta a novas ameaças e tecnologias emergentes.

Abordagem em Camadas

Segurança eficaz exige uma defesa em camadas, que inclui medidas físicas, técnicas e administrativas.

Treinamento e Conscientização

Fundamental para a cibersegurança é a educação contínua dos usuários sobre as melhores práticas de segurança.

Uso de Inteligência Artificial (AI)

AI e machine learning estão cada vez mais sendo incorporados para prever e identificar ameaças de forma proativa, analisando padrões de ataques e respondendo a eles mais rapidamente do que os humanos.

Regulamentações e Compliance

A cibersegurança é fortemente regulada por leis e normas que ditam como as informações devem ser protegidas. GDPR, HIPAA e outras regulamentações impõem padrões e penalidades para garantir a proteção de dados.

A cibersegurança moderna não só é definida pelo desenvolvimento e implementação de soluções defensivas, ela também incorpora uma abordagem proativa que inclui a simulação de ataques (pentesting) e a construção de ambientes resilientes capazes de se adaptar e responder a ameaças persistentes e evolutivas.

Ao mesmo tempo, os profissionais da área devem considerar as implicações éticas do uso de AI na cibersegurança, tanto para aprimorar as defesas quanto para antecipar e

se proteger contra o uso mal-intencionado da AI por agentes adversários.

A intersecção entre AI e cibersegurança é um território rico em potencial para o desenvolvimento de sistemas mais inteligentes e autônomos, mas também carrega a necessidade de vigilância constante e atualização de conhecimento para enfrentar os desafios que surgem com a evolução tecnológica.

Propósito e Objetivos

O propósito da Cybersecurity na camada de New Technology é robustecer a proteção aos ataques digitais, garantindo a segurança dos dados sensíveis e a resiliência dos sistemas de TI.

A integração da Inteligência Artificial (AI) em estratégias de segurança cibernética representa um avanço significativo, permitindo respostas mais ágeis e inteligentes a ameaças em evolução constante.

Objetivos da Cybersecurity integrada com AI:

- Detecção de Ameaças Melhorada: Utilizar algoritmos de AI para monitorar, detectar e analisar atividades suspeitas em tempo real, identificando ameaças potenciais com maior precisão.
- Resposta a Incidentes Acelerada: Desenvolver sistemas capazes de responder automaticamente a incidentes de segurança, reduzindo o tempo de reação e mitigando os danos potenciais.
- Automatização de Tarefas de Segurança: Implementar processos automatizados para atualizações de segurança e patches, diminuindo a carga operacional sobre as equipes de TI.
- Análise Preditiva de Segurança: Empregar modelos preditivos para prever e se preparar para ataques cibernéticos futuros, fortalecendo as defesas antes de qualquer comprometimento.
- Adaptação e Aprendizado Contínuo: Assegurar que os sistemas de segurança possam aprender com ataques anteriores e adaptar suas estratégias para enfrentar novos vetores de ataque.
- Inteligência Contra Ameaças: Colaborar na criação e no compartilhamento de inteligência sobre ameaças, aproveitando o conhecimento coletivo para melhorar a proteção.
- Governança e Conformidade: Reforçar políticas e procedimentos de segurança para garantir conformidade com regulamentos e padrões da

indústria.

- Educação e Conscientização: Promover a conscientização sobre cybersecurity em todos os níveis organizacionais, utilizando AI para personalizar treinamentos e simulações de segurança.
- Desenvolvimento de Talentos: Investir na formação e capacitação de profissionais de segurança em tecnologias emergentes e técnicas avançadas de AI.
- Segurança como Cultura Organizacional: Integrar práticas de segurança cibernética como um elemento fundamental da cultura organizacional.
- Parcerias Estratégicas: Estabelecer parcerias com fornecedores de tecnologia, instituições acadêmicas e organizações governamentais para desenvolver soluções inovadoras em cybersecurity.
- Proteção de Infraestruturas Críticas: Aplicar AI para proteger infraestruturas críticas e sistemas de controle industrial de ataques sofisticados.
- Análise Comportamental: Utilizar análise comportamental avançada para identificar desvios e prevenir ameaças internas.

Ao abraçar a AI como um componente crítico na estratégia de cybersecurity, as organizações podem não apenas reforçar suas defesas contra agentes maliciosos, mas também avançar em direção a uma postura proativa, onde antecipar e neutralizar riscos se torna parte integrante do ecossistema tecnológico.

Concluindo

A partir das previsões e estratégias delineadas, percebe-se uma clara necessidade de adaptação e inovação contínua no campo da cibersegurança.

As organizações devem priorizar não apenas a implementação de tecnologias avançadas, mas também a construção de uma cultura de segurança que coloque as pessoas no centro das estratégias.

Integrar a segurança cibernética com as metas de negócio e promover uma governança eficaz são passos essenciais para garantir que as organizações não apenas sobrevivam, mas prosperem em um ecossistema digital em constante evolução.

Pessoalmente, acredito que estas tendências refletem a evolução necessária nas

práticas de cibersegurança, onde a adaptabilidade e a humanização das estratégias são fundamentais para enfrentar os desafios futuros.

Além disso, a colaboração entre os líderes de TI e as partes interessadas em todos os níveis organizacionais será crucial para fomentar um ambiente seguro e resiliente.

A jornada para uma cibersegurança robusta é contínua e exige uma vigilância constante, inovação e, acima de tudo, uma compreensão profunda do valor da segurança centrada no ser humano e na privacidade como diferencial competitivo.

Arthur De Santis

Arthur De Santis é um executivo com mais de 20 anos de atuação na indústria de serviços financeiros, com destaque para bancos, processadoras de cartões, adquirentes e seguradoras, formando e liderando equipes e iniciativas ao longo de toda a cadeia de valor de Tecnologia da Informação.

The IT framework

O conteúdo apresentado neste website, incluindo o framework, é protegido por direitos autorais e é de propriedade exclusiva do CIO Codex. Isso inclui, mas não se limita a, textos, gráficos, marcas, logotipos, imagens, vídeos e demais materiais disponíveis no site. Qualquer reprodução, distribuição, ou utilização não autorizada desse conteúdo é estritamente proibida e sujeita às penalidades previstas na legislação aplicável