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

No cenário corporativo atual, a transformação digital ampliou significativamente os horizontes das empresas, mas também intensificou os desafios associados à segurança cibernética.

O aumento dos riscos de segurança, impulsionado pela expansão de sistemas e serviços e pela adoção de práticas digitais nas organizações, demanda um planejamento estratégico e operacional eficaz.

Líderes de TI estão na vanguarda, não apenas implementando soluções tecnológicas,

mas também promovendo discussões estratégicas essenciais para alinhar as políticas de segurança com os objetivos de negócio da empresa

Quando pensamos em Cybersecurity imediatamente pensamos em hackers e uma visão primordialmente tecnológica da coisa.

Mas quando se pensa na TI como um todo, existe um conjunto muito mais amplo de aspectos a serem considerados e endereçados.

Inclusive, amplo o suficiente para serem considerados e colocados na pauta de várias áreas dentro e fora da TI, em uma abrangência que vai muito além da “área de segurança”.

Aqui um artigo muito interessante do Gartner, ajudando a estruturar o que deve ser previsto em um roadmap de cybersecurity:

https://www.gartner.com/en/information-technology/trends/the-it-roadmap-for-cybersecurity

O artigo do Gartner

O artigo em análise detalha um plano estratégico robusto para o desenvolvimento de programas de segurança baseados em riscos, essenciais para suportar a agilidade e resiliência dos negócios.

Segundo a pesquisa, espera-se que até 2027, 75% dos funcionários de uma organização adquiram, modifiquem ou criem tecnologia fora da visibilidade do departamento de TI, um aumento significativo comparado aos 41% em 2022.

Tal cenário sublinha a necessidade imperativa de um programa contínuo de segurança, que não apenas atenda às regulamentações, mas também seja defensável e adaptável às rápidas mudanças do ambiente tecnológico.

As melhores práticas agregadas de milhares de interações com empresas revelam a importância de uma estrutura de governança forte e uma estratégia anual bem definida.

O envolvimento de líderes e equipes é crucial para o sucesso da implementação de qualquer iniciativa de cibersegurança, incluindo CISOs, líderes de aplicativos empresariais e engenharia de software, além de profissionais técnicos encarregados da infraestrutura e operações.

O roteiro proposto abrange vários estágios, desde a definição de estratégia e o desenvolvimento de um plano de ação até a execução inicial e a maturação do programa.

Cada etapa é detalhada com tarefas específicas, como avaliações de vulnerabilidade, testes de penetração, e o estabelecimento de uma arquitetura de segurança e políticas.

Além disso, a otimização contínua e a reavaliação do programa são enfatizadas para garantir sua eficácia e relevância continuada.

Componentes 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.

Etapas de um Roadmap de Cybersecurity

A elaboração de um programa de cibersegurança eficaz envolve uma série de etapas estruturadas que garantem a implementação adequada e a melhoria contínua das práticas de segurança.

Um roadmap de cibersegurança é composto por etapas críticas que incluem o alinhamento estratégico, o desenvolvimento de um plano de ação, a execução inicial, a maturação do programa e a reavaliação e otimização contínua.

Cada uma dessas fases é fundamental para garantir que a cibersegurança não apenas responda às necessidades atuais, mas também esteja preparada para os desafios futuros.

1. Align strategy

A primeira etapa crucial em qualquer roadmap de cibersegurança é o alinhamento estratégico.
Esta fase envolve definir claramente como a estratégia de cibersegurança se integra e suporta os objetivos gerais da empresa.

Inclui a identificação de prioridades de negócios, a avaliação de riscos existentes e potenciais, e o entendimento das metas de crescimento e resiliência da organização.

Durante esta etapa, é vital garantir que todas as partes interessadas, desde a alta direção até os executivos de TI, compreendam e apoiem a estratégia proposta.

O alinhamento estratégico facilita uma abordagem de segurança que é proativa e integrada à cultura e aos processos da empresa.

2. Develop action plan

Após estabelecer um alinhamento estratégico, o próximo passo é desenvolver um plano de ação detalhado.

Esta fase envolve a transformação da estratégia de cibersegurança em tarefas específicas, metas alcançáveis e cronogramas definidos.

O plano de ação deve abordar a priorização de riscos, a alocação de recursos, e estabelecer benchmarks claros para o sucesso.

Ele também deve incluir procedimentos para a implementação de tecnologias de segurança, políticas de governança, e programas de treinamento para funcionários.

O desenvolvimento de um plano de ação robusto e viável é essencial para a execução eficaz da estratégia de cibersegurança.

3. Initiate execution

A fase de iniciação da execução marca o começo da implementação prática do plano de ação.

Durante esta etapa, as políticas, processos e sistemas de cibersegurança são formalmente estabelecidos e postos em operação.

É crucial nesta fase garantir que todas as equipes envolvidas estejam devidamente informadas sobre suas responsabilidades e que os sistemas de monitoramento e resposta a incidentes estejam operacionais.

A iniciação efetiva é muitas vezes acompanhada de uma fase intensiva de testes e ajustes para assegurar que as soluções de segurança sejam eficazes e seguras antes de

se tornarem operacionais em escala completa.

4. Build and mature program

Após a implementação inicial, o foco muda para a construção e maturação do programa de cibersegurança.

Esta etapa envolve a ampliação e o aprofundamento das iniciativas de segurança para abranger todos os aspectos da organização.

A maturação do programa é um processo contínuo que inclui a melhoria das capacidades de detecção e resposta, a integração de novas tecnologias e práticas, e a fortificação contínua das defesas contra ameaças emergentes.

A construção e maturação são vitais para manter a eficácia do programa à medida que a organização e o cenário de ameaças evoluem.

5. Reassess and optimize

A última etapa do roadmap envolve a reavaliação e otimização contínua do programa de cibersegurança.

Esta fase é essencial para garantir que o programa permaneça relevante e eficaz diante das mudanças nas condições de mercado e avanços tecnológicos.

Inclui a revisão regular dos objetivos de segurança, a análise do desempenho do programa e a recalibração das estratégias conforme necessário.

A otimização contínua não apenas melhora a segurança, mas também assegura que a organização possa se adaptar de forma ágil e eficiente a novos desafios e oportunidades.

Integração das Iniciativas de Cibersegurança com Objetivos de

Negócio

A discussão estratégica entre líderes de TI e partes interessadas é vital para alinhar as iniciativas de cibersegurança com os objetivos de negócio da organização.

Esta integração é crucial para a adaptação às mudanças regulatórias e para a identificação e mitigação de ameaças emergentes.

A clareza nesses diálogos garante que todos os recursos de segurança estejam sincronizados com as metas estratégicas e operacionais.

Modernização dos Sistemas para Segurança

Questionar a modernidade dos sistemas de TI é fundamental para garantir sua segurança.
A transição para arquiteturas modernas, como as nuvens públicas e privadas, deve ser priorizada, pois integram a segurança diretamente na infraestrutura, fortalecendo a defesa contra ataques cibernéticos e alinhando a infraestrutura de TI com as práticas modernas de desenvolvimento de software.

Planejamento de Cenários de Ciberataques

Simulações e discussões de cenários de ciberataques são essenciais para avaliar e fortalecer a capacidade de resposta a incidentes.

Envolver gestores e funcionários em planejamentos regulares de resposta a incidentes enriquece a preparação da organização e estabelece procedimentos claros e eficazes para a gestão de crises.

Cultura de Segurança Organizacional

Promover uma cultura de segurança em todos os níveis da organização é fundamental.

Líderes devem incentivar práticas de segurança proativas, educando e capacitando funcionários a operar dentro de diretrizes claras de segurança. Uma cultura robusta de segurança acelera a inovação e protege os resultados do negócio.

Atualização Sobre Ameaças Emergentes

Manter-se atualizado sobre as ameaças emergentes permite que os líderes de segurança adaptem estratégias para enfrentar novos desafios.

Discussões diretas sobre tendências recentes em ameaças cibernéticas são cruciais para reorientar as estratégias de defesa e realocar recursos de TI para infraestruturas mais seguras, como serviços em nuvem.

Avaliação do Retorno sobre Investimento em Segurança

É crucial discutir como os investimentos em segurança estão protegendo ativos e reduzindo riscos.

Avaliar continuamente o retorno sobre o investimento ajuda a justificar os gastos e adaptar as estratégias à medida que o ambiente de ameaças evolui.

Melhorar a visibilidade e a gestão dos controles de segurança, processos e regulamentações maximiza o retorno sobre os investimentos em segurança.

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 – Principais conceitos e características de

Cybersecurity

A fim de prover alguma base teórica, listo a seguir uma pequena parte do conteúdo do CIO Codex Framework sobre esse tema.

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.
- **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.

Concluindo

As discussões em torno da segurança da informação não são meramente técnicas, afinal elas são essencialmente estratégicas e necessárias para a sustentabilidade do negócio.

A partir do que foi apresentado, considero que tais diálogos devem ser uma prática regular e engajar não apenas os líderes de TI, mas todos os executivos da empresa.

Estabelecer uma cultura de segurança robusta e responsiva não é apenas sobre implementar as melhores ferramentas, mas sobre integrar profundamente a segurança no ethos e nas operações diárias da empresa.

Afinal, num mundo onde as ameaças evoluem rapidamente, a adaptabilidade e o compromisso contínuo com a segurança são o que verdadeiramente protegerão nossos

ativos mais valiosos.

Julgo relevante reforçar a necessidade de manter essas conversas críticas em todos os níveis da organização, garantindo que a segurança seja percebida não como um custo, mas como um investimento essencial na resiliência e no futuro do negócio.

A abordagem da Gartner para a elaboração de um roteiro de cibersegurança destaca a necessidade de uma estratégia integrada que alie segurança e gestão de riscos ao crescimento e objetivos empresariais.

A partir da minha experiência reconheço a validade desta abordagem, que não apenas protege os recursos da empresa, mas também fortalece sua posição no mercado digital competitivo.

A implementação de um programa de cibersegurança robusto e defensável é indispensável para a sustentabilidade e sucesso a longo prazo de qualquer empresa no cenário digital atual.

Essencialmente, a cibersegurança deve ser vista não como um custo, mas como um investimento estratégico que propicia vantagens competitivas significativas.