RESILIÊNCIA CIBERNÉTICA E O TEMPO DO RANSOMWARE

POR QUE A MAIORIA DAS DEFESAS REAGE TARDE DEMAIS — E ONDE ESTÁ O VERDADEIRO PONTO DE RUPTURA

Fausto Bacchi Neto

1ª edição

APOIO:

BUNKER CYBER SECURITY

Security Snares

MASSIMA FROG

SUMÁRIO

PREFÁCIO

RESILIÊNCIA COMO DECISÃO ESTRATÉGICA EM UM MUNDO SOB ATAQUE

POR FABIANA TANAKA

O avanço do ransomware reposicionou a segurança da informação no centro das decisões estratégicas das organizações. O que antes era tratado como um desafio predominantemente técnico passou a impactar diretamente a continuidade dos negócios, a confiança de clientes, a estabilidade operacional e, em alguns setores, a própria vida humana. Este e-book surge nesse contexto, oferecendo uma reflexão profunda, prática e conectada à realidade.

Ao longo dos capítulos, Fausto Bacchi e os autores convidados exploram a resiliência cibernética como uma capacidade organizacional que vai além de ferramentas ou controles isolados. Trata-se de preparar pessoas, processos e tecnologias para operar sob pressão, responder com rapidez e preservar o controle mesmo diante de cenários adversos. O ransomware, apresentado aqui como um fenômeno econômico e estrutural, evidencia a urgência dessa mudança de mentalidade.

A obra nos convida a repensar o papel do tempo, da resposta a incidentes e da recuperação como fatores críticos para mitigar impactos. Em

um ambiente onde a detecção pode ocorrer tardiamente e a assimetria favorece os atacantes, a capacidade de interrupção imediata e de decisão consciente torna-se determinante. Preservar o negócio passa a ser tão relevante quanto proteger sistemas.

Outro mérito deste e-book está na abordagem integrada da resiliência. Os textos reforçam que ela não pertence a uma única área ou função, mas exige engajamento da alta liderança, governança clara e comunicação eficaz durante crises. Marcos regulatórios, indicadores de desempenho e exemplos setoriais, como o da saúde, ampliam a compreensão da resiliência como um tema estratégico, mensurável e essencial à sustentabilidade das organizações.

Por fim, esta obra de Fausto Bacchi e demais profissionais convidados valoriza o fator humano na cibersegurança. Decidir sob pressão, lidar com emoções e comunicar-se de forma responsável são competências tão críticas quanto qualquer tecnologia. Ao reunir diferentes visões e experiências, este e-book contribui para uma compreensão mais madura da ciber-resiliência e

oferece subsídios valiosos para líderes que precisam conduzir suas organizações em um cenário de ameaças constantes.

Que esta leitura provoque reflexão, fortaleça decisões e estimule práticas mais consistentes, colaborativas e conscientes frente aos desafios da segurança cibernética contemporânea.

Boa leitura.

Fabi Tanaka
CISO, Diretora de Cibersegurança e Proteção de Dados - Leroy Merlin Brasil

ilustração gerada com apoio do chatgpt

POR QUE RESILIÊNCIA CIBERNÉTICA SE TORNOU UM TEMA ESTRATÉGICO

AUTOR – FAUSTO BACCHI NETO

Escrevo este material movido menos por novidade tecnológica e mais por **preocupação prática.**

Ao longo dos últimos anos, acompanhando organizações de diferentes setores — indústria, serviços, saúde, educação e tecnologia — tornou-se evidente que o **ransomware** ocupa espaço recorrente nas agendas de executivos, conselhos e lideranças de negócio.

Hoje, não estamos falando apenas de dados indisponíveis. Falamos de hospitais com procedimentos adiados, cadeias produtivas interrompidas, serviços essenciais paralisados, impactos regulatórios e decisões críticas tomadas sob janelas de tempo extremamente curtas.

Relatórios globais indicam prejuízos anuais de dezenas de bilhões de dólares associados ao ransomware, considerando custos diretos e indiretos. Mais relevante do que o volume é o fato de que **organizações maduras, bem estruturadas e com investimentos consistentes em segurança continuam sendo afetadas.**

Essa realidade impõe uma reflexão inevitável:

Será que estamos protegendo os pontos certos, no momento certo?

Para ampliar essa reflexão, convidei executivos de cibersegurança que sempre atuaram na linha de frente da gestão de riscos e da resposta a incidentes. Nos capítulos bônus, eles compartilham experiências reais e perspectivas complementares sobre resiliência, decisão sob pressão e impacto ao negócio.

E minha motivação para escrever sobre resiliência cibernética nasce exatamente dessa pergunta. Em muitos incidentes que acompanhei, não houve ausência de controles. Havia processos, ferramentas, pessoas capacitadas e investimentos relevantes. Ainda assim, o impacto ocorreu. Não por negligência, mas por tempo.

Resiliência, no fim, não é negar o risco.

É estar preparado para não perder o controle quando ele se materializa.

CAPÍTULO 1

RANSOMWARE: UM FENÔMENO TÉCNICO, ECONÔMICO E ESTRUTURAL

AUTOR – FAUSTO BACCHI NETO

O ransomware nunca foi apenas um problema técnico. Desde suas primeiras manifestações, ele sempre combinou **execução tecnológica com motivação econômica**. O que mudou ao longo do tempo não foi a natureza do ataque, mas a **escala, a sofisticação e o contexto em que ele ocorre.**

Hoje, o ransomware opera em um ambiente significativamente mais complexo. Negócios cada vez mais digitais, infraestruturas híbridas, cadeias produtivas interconectadas, dependência de disponibilidade contínua e maior pressão regulatória ampliaram o impacto potencial de qualquer interrupção.

Nesse cenário, um ataque de ransomware bem-sucedido não afeta apenas sistemas. Ele compromete **operações, receitas, contratos, confiança do mercado e continuidade do negócio**. O custo do ataque deixa de ser pontual e passa a ser estrutural, propagando-se rapidamente por diferentes áreas da organização.

Paralelamente, os ataques tornaram-se mais sofisticados. Grupos de ransomware operam hoje com planejamento, persistência e

conhecimento profundo dos ambientes que atacam. Isso exige das organizações **mais recursos, mais preparo, mais estratégia e maior maturidade operacional** — nem sempre disponíveis no momento crítico.

Apesar dessa complexidade crescente, a lógica econômica da extorsão permanece clara. Para que o modelo de ransomware funcione, três elementos continuam sendo fundamentais:

1. **Interrupção real das operações**, afetando sistemas e serviços essenciais;
2. **Pressão operacional e psicológica**, reduzindo drasticamente o tempo disponível para decisão;
3. **Limitação de alternativas imediatas**, especialmente no curto prazo.

A criptografia dos arquivos segue sendo o mecanismo central que viabiliza esses fatores. Sem ela, o impacto é reduzido, a pressão diminui e o poder de negociação do atacante enfraquece.

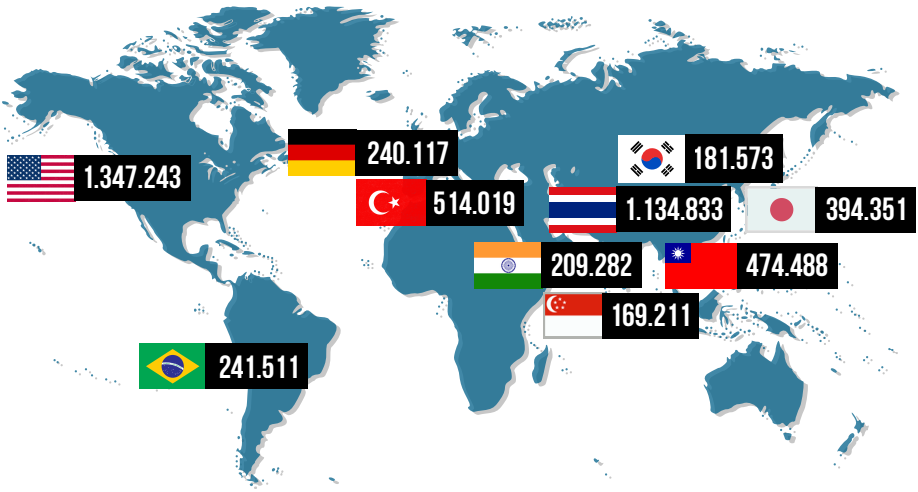
Do ponto de vista do ransomware, criptografar continua sendo vencer.

Essa dinâmica é amplamente sustentada por dados de mercado. Segundo o relatório **The State of Ransomware 2025**, da **Sophos**, o custo médio de recuperação de um ataque de ransomware — **excluindo qualquer valor de resgate pago** — atingiu **US$ 1,53 milhão**. Ainda assim, **49% das organizações vítimas acabaram pagando o resgate**, representando a segunda maior taxa de pagamento dos últimos seis anos. O valor médio exigido em pedidos de resgate chegou a **US$ 1,32 milhão**, evidenciando a dimensão econômica da ameaça. O relatório aponta ainda que **28% das organizações com dados criptografados sofreram exfiltração de informações**, ampliando o impacto para além da indisponibilidade operacional.

O **Ransomware Insights Report 2025**, da **Barracuda**, reforça esse cenário ao indicar que **57% das organizações sofreram ataques de ransomware bem-sucedidos nos últimos 12 meses**. Entre as vítimas, **32% pagaram resgate**, e **41% dessas organizações não conseguiram recuperar todos os seus dados**, mesmo após o pagamento. Embora **65% tenham conseguido restaurar informações a partir de backups**,

os efeitos ultrapassam a recuperação técnica: **25% das empresas afetadas perderam clientes existentes e novas oportunidades de negócio**, demonstrando que o impacto do ransomware se materializa diretamente na sustentabilidade e no crescimento das organizações.

Longe de ser um fenômeno restrito a determinados mercados, essa realidade também se manifesta de forma clara no Brasil. O **Trend 2025 Cyber Risk Report**, da **Trend Micro**, aponta **o Brasil entre os dez países mais atacados por ransomware**, reforçando que essa combinação de complexidade técnica, pressão econômica e impacto estrutural já faz parte do cotidiano das organizações nacionais.



CAPÍTULO 2

RESILIÊNCIA NÃO É EVITAR O ATAQUE

AUTOR – FAUSTO BACCHI NETO

Durante muitos anos, a segurança da informação foi estruturada com foco quase exclusivo na prevenção. O objetivo era claro: impedir que o ataque acontecesse. Firewalls, antivírus, IDS, EDR, XDR e diversas outras camadas foram implementadas com a expectativa de bloquear ameaças antes que qualquer impacto fosse percebido.

Essa abordagem produziu avanços importantes e continua sendo essencial. O que mudou foi o contexto em que essas defesas operam. Ambientes tornaram-se mais distribuídos, negócios mais digitais, cadeias mais interdependentes e a tolerância à indisponibilidade praticamente inexistente.

Ao mesmo tempo, a superfície de ataque passou a ser fortemente influenciada por **identidade**.

Credenciais comprometidas, privilégios excessivos, acessos persistentes e falhas na governança de identidades tornaram-se vetores recorrentes em ataques de ransomware, levando muitas organizações a fortalecer disciplinas como **IAM, PAM e, mais recentemente, ITDR**

como parte central de suas estratégias de prevenção.

Nesse cenário, a pergunta central já não pode ser apenas "como evitamos o ataque?". A questão que passa a orientar a estratégia é outra: **o que acontece com o negócio quando o ataque começa?**

Resiliência cibernética não é sinônimo de falha na prevenção. É o reconhecimento de que, mesmo com bons controles — incluindo camadas maduras de gestão de identidades e acessos, controle de privilégios e mecanismos de detecção de ameaças baseadas em identidade — o risco residual permanece. Ataques bem-sucedidos demonstram que, ainda que essas disciplinas sejam fundamentais para reduzir a probabilidade de comprometimento, **elas não eliminam completamente a possibilidade de avanço até o ponto de impacto.**

Essa mudança de perspectiva desloca o foco da segurança idealizada para a segurança possível. Do controle absoluto para o controle sob pressão.

Da promessa de inviolabilidade para a preparação realista frente ao incidente. Não se trata de abandonar a prevenção, nem de minimizar o valor de disciplinas como IAM, PAM ou ITDR, mas de reconhecer que, mesmo em ambientes maduros, **o ataque pode evoluir até um estágio em que a contenção inicial se torna necessária**.

Diante desse contexto, torna-se evidente que apostar exclusivamente na prevenção deixou de ser suficiente. **É necessário também estar preparado para agir proativamente no exato momento em que o ataque se inicia**, quando as camadas anteriores já foram superadas, contornadas ou exploradas de forma combinada.

É importante deixar claro, no entanto, que resiliência cibernética não se limita à capacidade de intervenção no início do ataque. Ela depende, de forma igualmente crítica, de **estratégias maduras de backup e disaster recovery**, capazes de restaurar ambientes que já sofreram impacto significativo. Essas camadas continuam sendo fundamentais para a continuidade do

negócio após um ataque bem-sucedido, especialmente quando a prevenção e a contenção inicial não foram suficientes.

A ênfase deste capítulo está em destacar um ponto frequentemente subestimado: **o intervalo entre a prevenção e a recuperação**.

É nesse espaço — quando o ataque já começou, mas ainda não devastou completamente o ambiente — que muitas organizações ainda carecem de mecanismos eficazes de resposta. Fortalecer essa camada intermediária é o que permite reduzir drasticamente o impacto operacional, preservar opções de decisão e evitar que um incidente técnico se transforme em uma crise de negócio.

CAPÍTULO 3

O TEMPO COMO FATOR CRÍTICO DE FALHA

AUTOR – FAUSTO BACCHI NETO

Grande parte das estratégias de segurança parte da suposição implícita de que haverá tempo suficiente para **detectar, analisar, correlacionar eventos e responder** de forma coordenada. Essa suposição sustenta boa parte das arquiteturas modernas de segurança.

No contexto do ransomware, porém, **nem sempre essa suposição se confirma.**

A dinâmica do ransomware impõe uma assimetria severa entre ataque e defesa. Enquanto o atacante precisa apenas de um ponto de entrada e de um curto intervalo para causar dano relevante, **a defesa depende de múltiplos sinais, validações, processos e até de decisões humanas para reagir de forma segura.**

Quando a criptografia se inicia, o impacto operacional começa a se materializar quase imediatamente. Sistemas ficam indisponíveis, usuários percebem falhas, processos críticos são interrompidos e a pressão sobre equipes técnicas e executivos aumenta rapidamente.

Nesse estágio, **o incidente deixa de ser apenas técnico e se transforma em uma crise operacional em tempo real.**

Em muitos cenários reais, o alerta não surge no início do ataque, mas quando o dano já está em curso. Mesmo em ambientes com monitoramento ativo, equipes estruturadas e processos definidos, o tempo necessário para confirmar o incidente, avaliar o escopo, decidir pela resposta adequada e executá-la pode ser maior do que a janela disponível para evitar impactos significativos.

Nesse contexto, **tempo deixa de ser apenas um recurso e passa a ser um fator crítico de falha.**

Resiliência, portanto, não é apenas a capacidade de reagir bem, mas de reagir cedo.

A perda dessa janela inicial compromete opções estratégicas. Quanto mais tempo o ataque avança sem interrupção, maiores se tornam os danos, mais limitadas ficam as alternativas de resposta e

mais difícil se torna manter o controle da situação. O custo não cresce de forma linear — ele se acumula, se propaga e se torna progressivamente mais difícil de conter.

Reduzir o intervalo entre o início do dano e a capacidade real de intervenção é o que separa um incidente contido de uma crise de grandes proporções.

ilustração gerada com apoio do chatgpt

CAPÍTULO 4

QUANDO A DETECÇÃO CHEGA DEPOIS DO IMPACTO

AUTOR – FAUSTO BACCHI NETO

As soluções modernas de EDR e XDR representam um avanço significativo na capacidade das organizações de identificar, investigar e responder a ameaças cibernéticas. Elas ampliaram a visibilidade sobre os ambientes, reduziram pontos cegos e elevaram o nível de maturidade defensiva do mercado.

Como profissional e empresário do setor de cibersegurança — e representante de uma solução de XDR líder de mercado — acredito fortemente no valor dessas plataformas e no papel estratégico que desempenham na proteção dos ambientes corporativos. Elas são, sem dúvida, uma das bases da defesa moderna e integram minhas recomendações a clientes.

Essas plataformas operam analisando múltiplas perspectivas do ambiente ao longo do tempo. Buscam identificar sinais de comprometimento como acessos indevidos, escalada de privilégios, movimentação lateral, execução de comandos suspeitos e a introdução de artefatos maliciosos. A partir da correlação desses eventos, constroem uma narrativa que indica a presença de um ataque em andamento.

Esse modelo é tecnicamente sólido e continua sendo essencial. O desafio surge quando o ataque não se manifesta de forma contínua, explícita ou ruidosa. Em muitos incidentes de ransomware, o artefato malicioso é introduzido no ambiente e permanece inerte por longos períodos, aguardando o momento mais oportuno para ser ativado.

Quando a criptografia começa, o ambiente já carrega um histórico fragmentado de eventos distribuídos no tempo. Para que a solução conclua que há um ataque em curso, ela precisa correlacionar retrospectivamente esses sinais, atribuir pesos, reduzir falsos positivos e atingir um grau mínimo de confiança estatística.

Esse processo leva tempo.

Com ransomware, esse tempo é escasso.

O impacto operacional ocorre antes que a narrativa esteja completamente formada. Sistemas começam a falhar, dados se tornam indisponíveis e a organização entra em modo de resposta sob pressão.

A detecção não falhou — ela simplesmente **chegou tarde demais para evitar o dano inicial**.

Essa não é uma limitação da tecnologia em si, mas do **modelo de atuação**. Abordagens baseadas em comportamento, inferência e probabilidade dependem, por definição, de observação e correlação ao longo do tempo. O ransomware explora exatamente esse intervalo.

Compreender essa limitação é essencial para evoluir a estratégia de resiliência cibernética. O desafio não está em substituir essas soluções — elas continuam sendo fundamentais —, mas em **complementá-las** com mecanismos capazes de atuar quando o ataque deixa de ser um padrão em formação e se transforma em um ato concreto de destruição.

CAPÍTULO 5

UMA ABORDAGEM FOCADA NO ATO, NÃO NO PADRÃO

AUTOR – FAUSTO BACCHI NETO

Grande parte das estratégias de segurança foi desenhada para **reconhecer padrões**. A detecção de ameaças, historicamente, depende da identificação de comportamentos suspeitos, da correlação de eventos e da reconstrução de narrativas que indiquem a presença de um ataque.

No contexto do ransomware, essa lógica encontra um limite importante.

Diferentemente de outras ameaças, o ransomware não depende de persistência prolongada para causar impacto. Seu objetivo central é **interromper operações por meio da criptografia dos dados**. Quando esse processo se inicia, o dano começa a se materializar imediatamente.

Nesse momento, a análise perde relevância frente à urgência da ação. A pergunta deixa de ser "**isso parece um ataque?**" e passa a ser uma decisão operacional imediata:
"**este ataque precisa ser interrompido.**"

Essa mudança de perspectiva altera a estratégia

defensiva profundamente. Em vez de aguardar a confirmação completa de um padrão, passa-se a atuar sobre o **ato concreto que produz o impacto.**

É nesse contexto que surgem **soluções especializadas na interrupção da criptografia maliciosa**. Diferentemente das plataformas focadas em detecção e resposta, essas abordagens não buscam reconstruir toda a cadeia do ataque. Seu papel é identificar, de forma objetiva, o início de um processo de criptografia anômala e **interrompê-lo imediatamente**, antes que o impacto se propague pelo ambiente.

Interromper a criptografia no momento em que ela começa não exige compreender toda a trajetória do invasor. Não depende de saber como o acesso foi obtido, quanto tempo o artefato permaneceu latente ou quais técnicas foram utilizadas até aquele ponto. Exige, antes de tudo, a capacidade de **reconhecer que o ato de criptografar dados de forma maliciosa é, por si só, inaceitável**.

Essa abordagem não concorre com EDR, XDR,

SIEM ou ferramentas de resposta. Ela atua em um **intervalo distinto**: o espaço crítico entre a prevenção que falhou e a recuperação que ainda não começou.

Ao bloquear o ataque no primeiro arquivo, o impacto operacional é drasticamente reduzido. Sistemas permanecem disponíveis, a pressão diminui e o tempo volta a ser um aliado. A organização deixa de reagir sob colapso e passa a conduzir o incidente com controle.

Resiliência, nesse contexto, não é apenas resistir.

É interromper o dano antes que ele se torne irreversível.

CONCLUSÃO

RESILIÊNCIA É PRESERVAR O CONTROLE

AUTOR – FAUSTO BACCHI NETO

O ransomware continua evoluindo não apenas em sofisticação técnica, mas em eficiência operacional. Ele explora assimetrias reais entre ataque e defesa, reduz janelas de decisão e transforma incidentes técnicos em crises de negócio em questão de minutos.

Ao longo deste e-book, ficou claro que a resiliência cibernética não se constrói em um único momento. Ela envolve **prevenção antes do ataque, capacidade de intervenção durante o ataque e recuperação após o impacto.** Todas essas camadas continuam sendo essenciais — e nenhuma, isoladamente, é suficiente.

O ponto central desta reflexão não é questionar o valor das defesas modernas, nem minimizar a importância de estratégias maduras de backup e disaster recovery. Pelo contrário. O que se buscou aqui foi iluminar um espaço historicamente negligenciado: o intervalo crítico entre a falha da prevenção e o início da recuperação.

É nesse intervalo que o ransomware vence ou perde.

Quando a criptografia começa, o tempo deixa de ser um recurso abundante e passa a ser um fator determinante. Decisões precisam ser tomadas sob pressão, com informação incompleta e impacto crescente. Reduzir o dano nesse momento não é apenas uma questão técnica — é uma decisão estratégica.

Resiliência, nesse contexto, não significa eliminar o risco. Significa **preservar o controle**. Ganhar tempo, manter sistemas operacionais, reduzir a pressão e ampliar o leque de opções disponíveis quando o incidente ocorre.

Organizações que incorporam essa visão deixam de reagir apenas após o colapso e passam a conduzir o incidente com racionalidade. Elas não dependem exclusivamente da sorte, nem de decisões tomadas no limite. Elas se preparam para **interromper o impacto antes que ele se torne irreversível**.

No cenário atual, essa capacidade deixou de ser um diferencial técnico. Ela se tornou um **elemento fundamental da continuidade do negócio**.

BÔNUS

RESILIÊNCIA EM CAMADAS: UMA VISÃO DE ECOSSISTEMA

CONVIDADO – MARCOS FLAVIO ANTONIAZZI

No mundo corporativo atual, tecnologia não é apenas um recurso — é o alicerce da operação e da competitividade. Sem estabilidade e capacidade tecnológica, não há condições de competir, expandir, gerar lucro ou, em muitos casos, sequer sobreviver.

Cibercriminosos perceberam que o verdadeiro valor está no negócio. O ransomware deixou de ser um ataque direcionado a computadores e passou a ser um ataque direto à continuidade do negócio. Hoje, ele paralisa operações, afeta o faturamento e compromete a confiança de clientes e parceiros, gerando impactos operacionais, financeiros e reputacionais.

Com ataques cada vez mais rápidos, automatizados e sofisticados, impulsionados pela inteligência artificial, a detecção e a prevenção se tornaram desafios exponenciais. Nesse cenário, não se trata mais de discutir se um ataque ocorrerá, mas quando. O risco não é técnico. É estratégico.

Por isso, a resiliência cibernética não é exclusivamente uma pauta do CISO. É um tema

de todo o ecossistema C-Level. Em caso de um ataque bem-sucedido, todos serão impactados — do CEO ao CFO. Estar preparado deixa de ser uma opção técnica e passa a ser uma decisão de negócio.

Resiliência exige mais do que uma arquitetura em camadas. Exige integração e visibilidade.

O primeiro objetivo é reduzir o risco, por meio de mecanismos de prevenção e detecção capazes de ampliar a visibilidade do ambiente e diminuir a probabilidade de comprometimentos iniciais. Soluções modernas de EDR e XDR cumprem um papel fundamental nesse estágio, elevando o nível médio de maturidade defensiva das organizações.

No entanto, a prevenção não elimina o risco residual. Quando um ataque ultrapassa essa camada inicial, a organização passa a depender de sua capacidade de conter o impacto e preservar opções de decisão. É nesse ponto que soluções especializadas, capazes de interromper a criptografia de ransomware, tornam-se

essenciais, permitindo a continuidade do negócio mesmo após uma tentativa de ataque.

Entre essas duas dimensões — evitar o ataque e recuperar-se dele — existe um intervalo crítico que frequentemente define o desfecho do incidente: o momento em que o ataque começa a causar dano real. É nesse espaço que atuam soluções focadas na interrupção imediata da criptografia maliciosa. Seu papel não é analisar o ataque em profundidade nem conduzir o processo de recuperação, mas impedir que o impacto se concretize, preservando a operação e devolvendo tempo à organização.

Quando essas camadas são pensadas como parte de um único ecossistema, o ransomware deixa de ser um evento binário — sucesso ou fracasso — e passa a ser um incidente controlável. O foco deixa de ser apenas reagir ao colapso e passa a ser preservar o controle, mesmo sob ataque.

Resiliência, nesse contexto, não é a soma de soluções. É a orquestração consciente e estratégica de capacidades desenhadas para atuar antes, durante e depois do ataque.

Envolve cultura, postura, tecnologia, processos e alianças estratégicas, formando um ecossistema preparado não apenas para evitar incidentes, mas para continuar operando quando eles ocorrerem.

ilustração gerada com apoio do chatgpt

BÔNUS

RESILIÊNCIA CIBERNÉTICA COMO CAPACIDADE DE NEGÓCIO

CONVIDADO – ANDRE VAKIMOTO

A evolução recente das boas práticas e dos marcos regulatórios mostra que a resiliência cibernética deixou de ser um tema estritamente técnico. Frameworks como o **NIST Cybersecurity Framework 2.0 (NIST CSF 2.0)** e regulações como o **DORA – Digital Operational Resilience Act,** da União Europeia, reforçam uma mudança fundamental: segurança não é mais medida apenas pela capacidade de prevenir incidentes, mas pela capacidade de **manter o negócio operando sob condições adversas**. O foco se desloca da proteção idealizada para a continuidade real, sob pressão, com impacto acontecendo e decisões precisando ser tomadas em tempo reduzido.

O **NIST CSF 2.0** consolida essa visão ao ampliar explicitamente a função **Governar** e reforça as funções de **Responder e Recuperar** como dimensões críticas para a sustentabilidade organizacional. O framework parte do reconhecimento de que falhas são inevitáveis e que maturidade não está em "não falhar", mas em **como a organização reage quando falha**. Indicadores como **MTTR (Mean Time to Recovery)** deixam de ser métricas

puramente técnicas e passam a refletir diretamente a capacidade de coordenação entre áreas, priorização de ativos críticos e tomada de decisão sob pressão durante incidentes reais.

O **DORA – Digital Operational Resilience Act** trata resiliência como um **requisito legal e operacional**, especialmente para o setor financeiro e seus provedores de tecnologia. O regulamento assume explicitamente que incidentes severos irão ocorrer e exige evidências de capacidade para **detectar, responder, conter e recuperar** dentro de janelas de tempo compatíveis com a criticidade dos serviços prestados. O foco não está em performance de desenvolvimento de software, mas em **estabilidade sistêmica, continuidade de serviços essenciais e redução de risco operacional em escala.**

O regulamento **DORA - Digital Operational Resilience Act** não deve ser confundido com o **DORA Metrics (DevOps Research and Assessment)** que se refere a um conjunto de indicadores de engenharia de software. Métricas como **CFR (Change Failure Rate)** e **LT**

(Lead Time for Changes) não são exigências diretas do regulamento europeu, mas podem ser utilizadas como **instrumentos complementares** para avaliar a capacidade operacional das organizações em responder rapidamente a falhas e incidentes.

Sob a ótica da resiliência cibernética, essas métricas ganham uma leitura de negócio. Uma alta taxa de falha em mudanças ou longos tempos para correção não indicam apenas ineficiência técnica, mas **fragilidade operacional**, aumento do risco sistêmico e menor capacidade de reação sob crise. Da mesma forma, métricas como **DF (Deployment Frequency)**, quando bem contextualizadas, podem indicar a capacidade da organização de aplicar correções emergenciais, ajustar controles e restaurar serviços sem paralisar o negócio.

A resiliência cibernética se consolida a partir da convergência entre governança, regulação e capacidade operacional mensurável, na qual o **NIST Cybersecurity Framework 2.0**, o **regulamento DORA** e o **DORA Metrics** exercem papéis complementares.

O NIST CSF 2.0 fornece a base conceitual e de governança ao reconhecer a inevitabilidade de falhas e reforçar as funções Governar, Responder e Recuperar como elementos centrais da maturidade organizacional; o DORA transforma essa visão em **exigência legal e operacional** ao demandar evidências concretas de capacidade de resposta e recuperação compatíveis com a criticidade dos serviços; e o DORA Metrics, embora não regulatório, oferece instrumentos práticos para mensurar a capacidade real de reação, correção e restauração sob pressão.

Integrados de forma consciente, esses referenciais permitem que a resiliência cibernética seja tratada não como um objetivo abstrato ou puramente técnico, mas como uma **capacidade organizacional governável, mensurável e diretamente** alinhada à **continuidade** e à **sustentabilidade do negócio**.

BÔNUS

CIBER-RESILIÊNCIA NO SETOR DE SAÚDE: UM IMPACTO SOCIAL

CONVIDADO – LEANDRO RIBEIRO

Falar de resiliência cibernética no setor de saúde é falar de um impacto direto na sociedade. Diferente de outros segmentos, o setor de saúde é acessado majoritariamente de forma preventiva, corretiva ou emergencial; afinal, ninguém busca esses serviços por lazer.

Quando discutimos prevenção e resiliência nesse contexto, precisamos focar no impacto real. Para ilustrar essa dimensão, convido você a refletir sobre os números de um hospital de grande porte:

- Quantas pessoas passam por um pronto-socorro em um único dia?
- Quantas cirurgias são realizadas?
- Qual é o volume anual de pacientes internados?
- Quantos exames são processados?

O Impacto em Números (Dados de 2024)

Para dar materialidade a essa discussão, compartilho os dados de uma instituição de São Paulo com aproximadamente 1.000 leitos (dados públicos de 2024), esses dados não são do

Hospital Sírio-Libanês.

Estes números ajudam a visualizar o impacto direto no paciente e na sociedade:

INDICADOR	VOLUME ANUAL	MÉDIA DIÁRIA
Atendimentos no Pronto-Socorro	366.000	~1.002 atendimentos
Internações	35.000 a 40.000	~100 internações
Cirurgias	35.900	~98 cirurgias
Exames (Clínicos e Imagens)	6.000.000	~16.438 exames

Estes números são impressionantes, não? Eles demonstram que um incidente de segurança ou uma falha de TI em um hospital não é apenas um "problema técnico". Trata-se de uma crise social com reflexos diretos no município e no estado, colocando vidas em risco e interrompendo o fluxo essencial de cuidados à saúde.

Impacto Humano e Segurança do Paciente

O risco assistencial em caso de interrupção sistêmica é imediato e crítico. Em um cenário de "papel e caneta", a margem de erro aumenta drasticamente, comprometendo a vida dos pacientes.

Consequências da Paralisia Sistêmica:

- **Paralisia Diagnóstica**: A interrupção de 16.438 exames diários retira dos médicos a base para decisões clínicas. Pacientes com suspeita de AVC ou infarto podem ter o tratamento atrasado pela falta de acesso aos resultados de exames.
- **Caos no Pronto-Socorro:** O fluxo de 1.002 atendimentos/dia gera um gargalo físico imediato. Sem sistemas de triagem digital e histórico clínico, o tempo de espera aumenta exponencialmente, impedindo a identificação rápida de casos críticos.
- **Risco Cirúrgico:** A suspensão de 98 cirurgias diárias compromete janelas terapêuticas estreitas de pacientes oncológicos e cardíacos. Além disso, perde-

se o controle automatizado de compatibilidade sanguínea e alergias a medicamentos, elevando o risco de eventos adversos graves.

Impacto Financeiro Direto e Indireto

O prejuízo financeiro em um hospital deste porte é multidimensional e vai além da interrupção imediata:

- **Perda de Receita Operacional:** A paralisia de procedimentos de alta complexidade pode representar perdas de milhões de reais por dia de inatividade.
- **Glosa e Faturamento:** Sem o registro digital dos materiais e procedimentos realizados nas 35.000 internações anuais, a instituição enfrenta dificuldades extremas para cobrança junto às operadoras, gerando um rombo no fluxo de caixa.
- **Custos de Remediação:** Incluem a contratação de perícia forense, restauração de backups e possíveis multas da LGPD, que podem chegar a 2% do faturamento (limitadas a R$ 50 milhões), além de

investimentos emergenciais em cibersegurança.

Dados de Mercado e Reflexão

Um estudo de 2023 da Universidade de Minnesota (EUA) revela a **gravidade de ataques de ransomware na saúde**:

- **Volume de Pacientes:** Redução de 17-26% na primeira semana.
- **Mortalidade:** Aumento de 35-41% entre pacientes já internados durante o ataque.
- **Receita Hospitalar:** Queda de 20-37%, com recuperação lenta em até 3 semanas.

Esses números não consideram custos adicionais com auditorias, novas tecnologias e resposta a incidentes.

A pergunta que fica para reflexão:

Será que estamos realmente preparados?

BÔNUS

FICÇÃO OU REALIDADE? HISTÓRIA FICTÍCIA BASEADA EM EXPERIÊNCIAS REAIS

CONVIDADO – ROGÉRIO GONÇALVES

Em tempos de Pandemia do COVID-19, o telefone toca, o Gerente de Segurança está em um compromisso pessoal em uma tranquila manhã no finalzinho do ano. Não deve ser nada grave!

- Estou terminando o meu compromisso, me liga em 20 minutos e falamos com mais calma, pode ser?

- Cara, o assunto é urgente! ***Estamos com 2 (dois) servidores criptografados! É um ataque de ransomware!*** *Tem até uma mensagem pedindo resgate em criptomoedas!*

O Gerente se lembra de que meses antes aconteceram várias reuniões e debates pensando nesse tipo de situação, e como seria acionar o botão de "pânico" em um incidente mais grave. Naquele tempo, "pipocavam" ataques de ransomware em diversas empresas brasileiras, um cenário parecido com o que acontece atualmente (2025).

- O primeiro procedimento será o seguinte!...."baixa" todo o ambiente produtivo que possa estar

comprometido ou se conecte com esses servidores, não podemos correr o risco do ransomware se espalhar.

O gerente dava essas instruções ao seu interlocutor voltando para casa e dirigindo com um aperto no peito, pois sabia que essa decisão causaria impactos imediatos na empresa.

*- Sim o time de TI já está "baixando" os servidores e já criamos uma "**sala de guerra**" para que o time técnico e os fornecedores possam atuar em conjunto.*

O ambiente afetado era razoavelmente importante para aquela organização (não era crítico), mas como não se tinha ideia da extensão

ilustração gerada com apoio do chatgpt

do ataque e nem um mapa confiável das interconexões entre os ambientes, a decisão foi desligar tudo o que pudesse ser acessado a partir daqueles dois servidores.

Obviamente, uma decisão como essa traz impactos visíveis ao negócio e tem potencial de ampliar o incidente transformando-o rapidamente em uma crise. Aplicações iriam parar, o site institucional ficaria fora do ar, o faturamento e os sistemas administrativos também, as pessoas tanto de dentro como de fora da organização seriam impactadas imediatamente.

Não é exatamente o que dizem as boas práticas para contenção de um incidente, mas é o que se tinha "na mão" para se evitar uma contaminação generalizada dos ambientes tecnológicos e consequentemente uma crise ainda maior e totalmente fora de controle, pensou o gerente.

Na sala de guerra havia vários técnicos, fornecedores e alguns gestores de TI, todos comprometidos em ajudar, mas sem uma direção clara do que fazer naquela situação. Começam as

perguntas para mapeamento do cenário:

- Nós sabemos se há outros ambientes contaminados?

- Não!

- Temos informações de como o ransomware entrou?

- Não!

- Sabemos se o backup do ambiente contaminado está integro?

- Não!

- Algum profissional experiente do fornecedor pode ajudar nessa crise?

- Claro! O Nicholas irá nos ajudar!

*- Temos **backup** do ambiente produtivo?*

*- **Sim, mas não fizemos testes de restauração**, ou seja, não temos certeza se tudo irá funcionar,*

portanto, não dá para "cravarmos" qual será ponto de restauração de cada ambiente. Pode ser o backup de ontem, pode ser o backup de 1 semana atrás...

A última resposta deixou o gerente mais preocupado! Como contar para a direção da empresa que além de tirar os sistemas do ar, não se tinha certeza de qual seria a posição (RPO) que eles iriam voltar após o incidente?

O gerente se lembrou de que alguns meses antes, eventos "não usuais" haviam ocorrido.... mudanças não autorizadas sem explicação, arquivos "estranhos" apareceram em alguns servidores, e até um suposto "hacker do bem" mandou mensagens para os executivos da empresa, dizendo que havia encontrado uma vulnerabilidade crítica no app da organização e pedindo pagamento adiantando em criptomoedas para revelar os seus "segredos". Será que algum desses eventos eram um sinal do que estava acontecendo naquele dia?

Enquanto o gerente refletia sobre o passado, o profissional experiente do fornecedor faz uma pergunta objetiva:

- Quem irá liderar a sala da guerra? Vocês ou nós?

- Vocês lideram a sala e eu lidero as conversas com as áreas de negócio e o reporte ao board, disse o gerente.

Pausa na nossa história! Há uma premissa que vem do mundo militar e que é comentada como uma das diversas causas da derrota dos nazistas na 2ª Guerra Mundial: a Cadeia de comando em uma guerra precisa ser clara! Em uma crise corporativa ou em uma campanha militar, essa premissa é fundamental para respostas rápidas e coordenadas, segurança dos envolvidos e principalmente eficiência! Vejam que o nosso "herói", o Gerente de Segurança, foi questionado e teve que tomar uma decisão importante de forma improvisada! Uma cadeia de comando clara (ou na linguagem corporativa papéis e responsabilidades) é parte essencial do processo de Gestão de Crises.

Em paralelo, começou a acontecer uma reunião com as áreas de negócio mais afetadas na crise, incluindo atendimento ao cliente, marketing, financeiro e RH que acabou virando um improvisado (mas bastante colaborativo) Comitê

de Crise:

- O que iremos comunicar para o time interno e para o mundo externo (clientes, fornecedores e parceiros)?

Pausa de novo! Antes de dizer qual será a decisão do agora Comitê de Crise, é importante salientar que aqui estamos diante do grande dilema da comunicação nas crises. Se falarmos abertamente que estamos sofrendo um ataque de ransomware, seremos transparentes, ganharemos empatia das pessoas, mas ao mesmo tempo virão as inevitáveis perguntas: Os meus dados estão seguros com a sua empresa? Quando os sistemas voltarão a funcionar? Vocês não investem em segurança? A outra estratégia, é não dizer muitos detalhes, até que se tenha alguma clareza do que está acontecendo. A contrapartida dessa estratégia, entretanto, será a acusação de falta de transparência da organização perante o mercado, os clientes, fornecedores, etc. Em uma crise, além do tempo de resposta , o controle da narrativa também é fator crítico pois, é melhor tomar "as rédeas do cavalo bravo, do que deixar que ele te derrube com boatos ou fake news".

- Vamos preparar uma comunicação externa dizendo que estamos sofrendo instabilidades sistêmicas e que nosso time já está trabalhando para normalizar a situação. Para o público interno, fora das atividades críticas, a orientação será desligar o computador hoje! Não será pago nenhum resgate ao criminoso.

Outro contexto importante de explicar: em tempos onde ainda não se tinham ferramentas eficazes para detecção e resposta a incidentes e com um SOC (Centro de Operações de Segurança) incipiente, pedir aos funcionários fora das atividades críticas para se desconectarem, era parte de uma estratégia de contenção de danos, pois não se sabia se havia estações de trabalho contaminadas, e na nossa história que se passa em tempos de pandemia, toda a força de trabalho atuava 100% remota impossibilitando ações presenciais do Service Desk.

- No final do dia será feita uma reunião com a alta direção da empresa para reporte e avaliação da crise, o presidente da empresa irá conduzir, pois entende a importância da segurança e os riscos que a organização está correndo.

Após várias discussões na Sala de Guerra e no Comitê de Crise, surgem as medidas de resposta que seriam aprovadas pela direção da empresa que mesmo diante da inevitável pressão do tempo, assumiu a responsabilidade delas junto ao time técnico:

- **Medida 1:** Já temos testado e instalado em algumas máquinas um ótimo EDR (Endpoint Detection and Response) portanto, vamos instalar esse software em todas as estações de trabalho e servidores;
- **Medida 2:** Os servidores contaminados serão refeitos com os dados do último backup, mas para reduzir o risco de recontaminação, esse ambiente "novo" ficará isolado para ser testado com ferramentas de segurança antes de virar novamente ambiente produtivo;
- **Medida 3:** Todos os outros servidores "baixados" só voltam para produção quando tivermos certeza de que o EDR está instalado e funcionando corretamente, eles também deverão passar pelos testes de segurança.

Como não temos um relatório de **BIA (Business Impact Analysis)**, a ordem de volta dos ambientes será de acordo com o tempo de restore e dos testes de segurança. Se terminou e está tudo "limpo", pode subir!

- **Medida 4**: Chamem a Perícia! Precisamos de um especialista para investigar a origem do incidente;
- **Medida 5**: Chamem o Jurídico! Precisamos formalizar um boletim de ocorrência e adotar as medidas legais que forem necessárias para defender a organização de eventuais prejuízos, questões contratuais administrativas ou regulatórias;
- **Medida 6**: Reportes de hora em hora via Teams e 03 reuniões diárias de no máximo 30 minutos para acompanhamento das medidas técnicas;
- **Medida 7**: Reunião diária de Ponto de situação com o board e presidência;
- **Medida 8**: No comitê de crise mediremos os impactos nos negócios, as medidas jurídicas e a "temperatura" externa da reputação da organização (clientes, fornecedores, redes sociais);

- **Medida 9:** Concluam a subida do SOC para melhorarmos a detecção e resposta a novos incidentes;
- **Bônus:** Negociação do prazo de pagamento de parceiros, priorização de pagamento de clientes, mensagens personalizadas para clientes relevantes ou mais afetados com envolvimento do time comercial, reportes diários do nível de satisfação (NPS) dos clientes.

As medidas foram colocadas em prática e os ambientes foram gradualmente retornando ao normal. A recuperação completa, demorou mais de 1 mês para ser concluída. Apesar da relativa "rapidez" para recuperação dos sistemas transacionais, sistemas de informações gerenciais (BI) demoraram mais, pois muitas configurações não eram documentadas já que não eram considerados "sistemas críticos".

O plano de resposta foi improvisado, mas executado com sucesso devido a cultura de colaboração existente na empresa e o apoio da alta direção. Um final feliz para um início ruim e com diversas falhas básicas de controles de

segurança.

Uma crise traz vários elementos humanos como distância ou rivalidade entre pessoas, falta de entendimento do que está acontecendo, emoções (raiva, indiferença, desespero), dilemas éticos na comunicação, pressão por respostas rápidas a fatos que não estão claros, profissionais em posição defensiva pois sentem que seus empregos estão ameaçados, falta de objetividade, falta de coragem para tomada de decisões e pessimismo.

Como já explorado no capítulo 3, o tempo de resposta é o fator crítico que separa um incidente contido ou controlado de uma crise de grandes proporções. Também comentei que o controle da narrativa é outro fator crítico. Agora imaginem a condução desses fatores críticos no meio desse caldeirão de elementos humanos? Quando uma crise acontece, há um roteiro que se repete e que não é tecnológico, é fundamentalmente humano.

Aspectos que considero fundamentais para a sobrevivência de uma organização em um ataque

de ransomware, e parte importante da resiliência cibernética:

1. **Ter o melhor inventário possível** e o máximo de **processos**, **ferramentas** e **pessoas** para uma rápida detecção e resposta a anomalias. Isso teria evitado em nossa história a estratégia de ter que baixar vários ambientes por não se ter ideia do que estava comprometido. Se as defesas iniciais não contiveram o ataque, vamos atuar rapidamente antes da crise maior!
2. A base do processo de resposta sempre será o **Plano de Gestão de Incidentes de Segurança** conectado a um **Plano de Continuidade de Negócios** , com priorizações e responsabilidades claras! Não se pode ter dúvida de quem lidera a sala de crise, de quem executa o que, dos procedimentos e da ordem de retorno dos ambientes tecnológicos "validada" pelo negócio.
3. **Ensaiar, testar, ter mensagens prontas para diferentes cenários**: o pior momento para se discutir a comunicação e/ou protocolos de resposta é no meio da crise.

Pequenos ajustes podem ser feitos de acordo com as circunstâncias, mas a ideia central tem que ser discutida previamente.

4. **Comunicação, comunicação, comunicação!**
5. **Apoio da alta gestão.** Esse é o ponto positivo ilustrado na nossa história, pois houve comprometimento das demais áreas da empresa e apoio direto do presidente durante a crise mostrando maturidade e reforçando a mensagem de que todos são responsáveis pela continuidade do negócio.

Em uma simulação de ataque de ransomware que participei recentemente, o CISO (Executivo responsável pela Segurança) foi demitido no meio da crise por pressão dos acionistas!

Isso mostra aquela necessidade humana (e errada!) de se achar um culpado pela tempestade quando se está em um barco no meio do mar, ao invés de se tentar controlar as velas, proteger o barco e a tripulação.

FONTES E REFERÊNCIAS

Este capítulo reúne algumas fontes externas relevantes para quem deseja aprofundar a análise de ransomware no contexto atual — estudos independentes, relatórios globais e pesquisas amplamente citadas pela comunidade de segurança cibernética.

As referências incluem pesquisa quantitativa, impacto econômico, tendências de ataque e insights estratégicos usados ao longo deste e-book.

Trend 2025 Cyber Risk Report (Trend Micro)
https://documents.trendmicro.com/images/TEx/articles/Research-Risk-Report-2025.pdf

Relatório do custo das violações de dados 2025 (IBM)
https://www.ibm.com/reports/data-breach

2025 Data Breach Investigations Report (Verizon Business)
https://www.verizon.com/business/resources/reports/dbir/

The State of Ransomware Q32025 (Checkpoint)
https://research.checkpoint.com/2025/the-state-of-ransomware-q3-2025/

Ransomware Report 2025: Building Resilience Amid a Volatile Threat Landscape (Akamai)
https://www.akamai.com/lp/soti/ransomware-trends-2025

Ransomware Statistics for 2025 (Ransom.Live)
https://www.ransomware.live/stats

The State of Ransomware 2025 (Sophos)
https://www.sophos.com/en-us/content/state-of-ransomware

Ransomware Insights Report 2025 (Barracuda)
https://pt.barracuda.com/reports/the-ransomware-insights-report-2025

SOBRE OS APOIADORES DO E-BOOK

Este e-book foi produzido de forma independente, pelo autor e convidados, com o apoio de organizações que atuam no ecossistema de **resiliência cibernética**, contribuindo para a discussão técnica, estratégica e de negócio sobre o enfrentamento ao **ransomware**:

SECURITY SNARES

Fabricante de software especializado em soluções de interrupção de criptografia maliciosa, atuando de forma complementar às estratégias tradicionais de prevenção, detecção e recuperação. Sua abordagem é focada na contenção do impacto do ransomware no momento em que ele se inicia.
linkedin.com/company/securitysnares/

BUNKER CYBER SECURITY

Distribuidor especializado em soluções de cibersegurança, responsável pela introdução e desenvolvimento de tecnologias inovadoras no mercado brasileiro, com foco em resiliência, proteção de ambientes críticos e resposta a incidentes.
linkedin.com/company/bunker-cyber-security/

MASSIMA FROG

Consultoria especializada em governança, segurança da informação, cibersegurança e resiliência digital, apoiando organizações na construção de estratégias integradas de proteção, continuidade e resposta a incidentes.

linkedin.com/company/massimafrog/

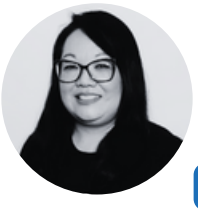
SOBRE O AUTOR E CONVIDADOS

O AUTOR

Fausto Bacchi Neto é executivo empreendedor no setor de tecnologia e cibersegurança, com mais de 36 anos de carreira em ambientes corporativos. Desde 2017 é conselheiro da ABES – Associação Brasileira das Empresas de Software.

Sua visão sobre resiliência cibernética foi construída principalmente a partir da observação prática de incidentes reais, de conversas recorrentes com CISOs, líderes de tecnologia e executivos, e da atuação direta em projetos de segurança e resposta a crises. Essa vivência mostrou que, muitas vezes, o problema não é a falta de controles, mas o tempo disponível para reagir ao risco que se materializa.

Atualmente, é sócio e diretor executivo da Massima Frog, consultoria especializada em cibersegurança, governança e resiliência digital, apoiando organizações na construção de estratégias que vão além da prevenção e priorizam a continuidade do negócio.



PREFÁCIO

Fabi Tanaka é CISO e Diretora de Cibersegurança e Proteção de Dados da Leroy Merlin Brasil, com mais de 18 anos de atuação em segurança da informação, privacidade e gestão de riscos em ambientes corporativos de alta criticidade.

Ao longo da carreira, liderou programas de cibersegurança, resposta a incidentes, SOC, CSIRT e iniciativas de privacidade e conformidade regulatória, sempre com foco na continuidade dos negócios e na tomada de decisão sob pressão. Atuou em organizações de grande porte nos setores de varejo, saúde, serviços financeiros e meios de pagamento, participando também de fóruns e comitês globais como PCI DSS

Reconhecida como Top Global CISO 2024 pela Cyber Defense Magazine, Fabi é conselheira da Rede Líderes Digitais e membro da WOMCY – LatAm Women in Cybersecurity, contribuindo ativamente para o fortalecimento do ecossistema e da liderança em cibersegurança.

CONVIDADO

Marcos Flávio Antoniazzi é sócio-diretor da Bunker Cyber Security, empresa especializada em cibersegurança com atuação focada em resiliência digital e proteção contra ransomware.

Possui sólida experiência no mercado de segurança da informação, trabalhando diretamente com organizações na estruturação de estratégias de defesa em camadas, resposta a incidentes e elevação da maturidade cibernética.

Ao longo de sua trajetória, tem acompanhado de perto a evolução das ameaças e os desafios enfrentados por equipes de segurança em ambientes cada vez mais complexos. Neste e-book, contribui com uma visão de ecossistema e resiliência aplicada, reforçando a importância de abordagens integradas que vão além da prevenção e consideram o impacto real ao negócio.

CONVIDADO

Leandro Ribeiro é Gerente de de Segurança da Informação do Hospital Sírio-Libanês, Diretor de Cyber Segurança da ABCIS e embaixador da Health-ISAC para o Brasil, atuando diretamente na proteção de ambientes críticos de saúde, onde disponibilidade, integridade e segurança da informação são fatores essenciais para a continuidade do cuidado e da operação hospitalar.

Com forte atuação prática em governança, gestão de riscos e resposta a incidentes, Leandro traz para este e-book uma visão aplicada da resiliência cibernética em contextos de alta criticidade, contribuindo com reflexões que conectam segurança da informação, impacto operacional e responsabilidade institucional em setores onde o tempo de resposta é determinante.

CONVIDADO

Andre Vakimoto com sólida trajetória em posições de liderança em segurança cibernética em organizações de diferentes setores, como Banco Carrefour, Dotz, Aché Laboratórios, Central Nacional Unimed, Sompo Seguros e Andrade Gutierrez.

Sua experiência transita entre ambientes financeiros, industriais e de serviços, sempre com foco em arquitetura, governança, riscos, conformidade e alinhamento da segurança aos objetivos do negócio.

Neste e-book, Andre contribui com uma análise que relaciona o tema da resiliência cibernética a frameworks amplamente adotados, como o NIST Cybersecurity Framework (CSF) e o DORA, explorando como estruturas de referência podem apoiar decisões estratégicas, fortalecer a governança e tornar a segurança mais integrada às demandas regulatórias e de negócio.

CONVIDADO

Rogerio Gonçalves atuou como Cybersecurity and Fraud Prevention Manager da VR Benefícios, com experiência focada na proteção de ambientes corporativos, prevenção a fraudes e mitigação de riscos cibernéticos em operações de grande escala. Sua trajetória combina segurança da informação, gestão de riscos e visão prática sobre ameaças digitais que impactam diretamente o negócio.

No capítulo bônus deste e-book, Rogerio contribui com uma abordagem orientada à experiência de campo, conectando os conceitos de resiliência cibernética à realidade operacional das organizações e aos desafios enfrentados por equipes de segurança no dia a dia, especialmente diante de ataques sofisticados e cenários de pressão.

AGRADECIMENTOS

AGRADECIMENTOS

Este e-book só se tornou possível graças à colaboração generosa de profissionais que atuam diariamente na linha de frente da cibersegurança, da governança e da proteção de operações críticas.

A todos os autores convidados, apoiadores e colaboradores que contribuíram com seu tempo, conhecimento e visão, deixo aqui meu sincero agradecimento.

Resiliência cibernética não é um conceito abstrato nem um exercício teórico. Ela se manifesta quando um incidente acontece, quando o tempo se torna escasso e quando decisões precisam ser tomadas, sob pressão, com impacto direto no negócio.

As reflexões reunidas neste e-book foram construídas a partir de experiências reais, de projetos, incidentes e diálogos com líderes que enfrentam esse cenário na prática. A intenção foi provocar uma visão mais realista, responsável e

estratégica sobre como as organizações podem se preparar para esses momentos.

Se esta leitura provocar reflexão ou contribuir de alguma forma para sua atuação profissional, sinta-se à vontade para compartilhá-la com outros líderes e profissionais que também enfrentam esses desafios no dia a dia.

Muito obrigado!

Fausto Bacchi Neto

Resiliência Cibernética e o Tempo do Ransomware

APOIO: