ESTUDO DE CASO SOBRE A IMPORTÂNCIA DO PLANO DE CONTINUIDADE DE NEGÓCIOS APÓS UM ATAQUE DE *RANSOMWARE*

CASE STUDY ON THE IMPORTANCE OF A BUSINESS CONTINUITY PLAN AFTER A *RANSOMWARE* ATTACK

Camila Teixeira dos Santos Menchão
Faculdade de Tecnologia de Santana de Parnaíba
camila.menchao@fatec.sp.gov.br

Marcelo Santiago de Almeida
Faculdade de Tecnologia de Santana de Parnaíba
marcelo.almeida34@fatec.sp.gov.br

Irapuan Glória Junior
Faculdade de Tecnologia de Santana Parnaíba
irapuan.gloriajr@fatec.sp.gov.br

Resumo

Um plano de continuidade de negócios (PCN) é um documento que possui medidas e estratégias elaboradas por uma organização para garantir a continuidade de suas operações em situações de interrupções. O *Ransomware* é um tipo de *malware* que sequestra os arquivos de um computador, exigindo um pagamento para liberá-los, em que por meio de técnicas de engenharia social, exploração de vulnerabilidades em sistemas operacionais e aplicativos, os cibercriminosos têm sido capazes de lançar ataques *Ransomware* cada vez mais perigosos, incluindo a propagação por meio de e-mails de *phishing* e *download* de *software* maliciosos. A pesquisa possui natureza qualitativa com a utilização da metodologia de estudo de caso único, com o objetivo de identificar qual a importância do plano de continuidade de negócios após um ataque de *Ransomware*. O resultado é que graças ao PCN a empresa-alpha passou pelo ataque sem maiores danos. A contribuição prática foca em fornecer sugestões de melhoria e de mitigação sobre o Plano de Continuidade de Negócios, permitindo que os gestores as incorporem em suas empresas. As contribuições teóricas destacam a importância do plano de continuidade de negócios em relação à um ataque de *Ransomware*.

Palavras-chave: Plano de Continuidade de Negócios, *Ransomware*, Concreteiras, Cibersegurança.

Abstract

A business continuity plan is a document that contains measures and strategies drawn up by an organization to guarantee the continuity of its operations in the event of an interruption. Ransomware is a type of malware that hijacks a computer's files, demanding payment to release them. Through social engineering techniques, exploitation of vulnerabilities in operating systems and applications, cybercriminals have been able to launch increasingly dangerous Ransomware attacks, including propagation through phishing emails and malicious software downloads. The research is qualitative in nature, using a single case study methodology to identify the importance of a business continuity plan after a Ransomware attack. The result is that thanks to the PCN the Empresa-Alpha came through the attack without major damage. The practical contribution focuses on providing suggestions for improving and mitigating the Business Continuity Plan, allowing managers to incorporate them into their companies. The theoretical contributions highlight the importance of the business continuity plan in relation to a Ransomware attack.

Keywords*: Continuity Plan, Ransomware, Concrete Plants, Cybersecurity.*

1. Introdução

O Plano de Continuidade de Negócios (PCN) é importante para garantir resiliência empresarial diante de interrupções, auxilia na gestão de riscos e conformidade com melhores práticas, aumentando a confiança dos clientes, protegendo a reputação da organização e minimizando custos (WEILL; ROSS, 2020). Além disso, atende requisitos legais, oferece agilidade na crise e promove aprendizado contínuo (FONTES, 2017). Em essência, o PCN é um sólido framework para assegurar a continuidade operacional e mitigar riscos (ISO, 2013), como um ataque de *Ransomware*.

O *Ransomware* é uma manifestação de código ou aplicativo malicioso, reconhecido como malware, com a finalidade de extorquir fundos de outros indivíduos. Inicialmente, o criminoso penetra e assume o controle dos dispositivos pertencentes a um usuário, dificultando a entrada em seus arquivos, a exemplo de imagens, planilhas e outros registros documentais. Em contrapartida pela restituição do acesso a vítima, o criminoso exige o pagamento de uma quantia determinada e estipula um prazo para cumprimento (MARION; TWEDE, 2020).

Este trabalho possui como questão de pesquisa: "Como o Plano de Continuidade de Negócios pode contribuir para a restauração dos serviços em uma empresa do setor de construção após um ataque *Ransomware*?". Os objetivos são: (1) Identificar a estrutura tecnológica da empresa atacada; (2) Levantar como foi o ataque sofrido pela Empresa-

Alpha; (3) Apresentar as medidas realizadas pela empresa para restaurar o ambiente; e (4) Sugestões para a melhoria do PCN.

2. Referencial Teórico

2.1. Plano de Continuidade de Negócios

O plano de continuidade de negócios é um processo que busca garantir a resiliência de uma organização contra danos e interrupções, permitindo atingir metas, restabelecer atividades e lidar com diversos tipos de interrupções. Isso é alcançado por meio de uma estrutura estratégica e operacional adequada (WEILL; ROSS, 2020).

Outra definição que pode ser encontrada é que o PCN é um documento que mostra o que uma empresa deve fazer quando houver interrupções. Ele ajuda a empresa a lidar com diferentes problemas que podem acontecer e diz o que fazer em cada situação. Também verifica se existem boas maneiras de lidar com esses problemas e sugere novas maneiras se for preciso. Isso ajuda a empresa a manter o controle das situações difíceis (FONTES, 2017).

Para conseguir um melhor aproveitamento de toda gestão de continuidade de negócios (GCN), é necessário a definição de um PCN, sendo este otimizado por boas práticas (ISO, 2013), tais como *Information Technology Infrastructure Library* (ITIL, 2019), *Control Objectives for Information and Related Technologies* (COBIT, 2021), *Balanced Scorecard* (BSC, 2021) e *Business Impact Analysis* (BIA, 2023).

O plano de continuidade de negócio deve ser desenvolvido tendo em conta as especificidades da empresa, focando-se nas suas reais necessidades para garantir a eficiência operacional e minimizar os custos financeiros. Essencialmente, o PCN visa atender aos requisitos dos processos de negócios, incluindo testes de contingências integrados com locais de negócios, fornecedores críticos e conexões externas para atingir os tempos de recuperação exigidos pela criticidade do negócio (ROSINI; NEUBARTH, 2023).

2.2. *Ransomware*

O *Ransomware* é um tipo de *malware* que sequestra os arquivos de um computador, exigindo um pagamento para liberá-los, em que por meio de técnicas de engenharia social, exploração de vulnerabilidades em sistemas operacionais e aplicativos (INSIDE, 2023). Os cibercriminosos têm sido capazes de lançar ataques *Ransomware* cada vez mais perigosos, incluindo a propagação por meio de e-mails de *phishing* e *download* de *software* maliciosos (SILVA; GLÓRIA JÚNIOR, 2023).

Verificando as variantes de *Ransomware*, pode-se identificar cerca de nove, sendo elas: (1) *Crypto malware*: Explora uma vulnerabilidade do Windows, deixando a máquina exposta para criptografar os arquivos e pedir resgates (BURDOVA, 2022); (2) *Locker*: Infecta o SO impossibilitando acesso a todos os arquivos e aplicativos (MOURA, 2022); (3) *Scareware*: Age como um antivírus falso afirmando ter encontrado problemas e solicitando dinheiro para resolver, enchendo a tela de mensagens pop-up (RAMOS, 2021); (4) *Doxware*: Ameaça publicar as informações do usuário on-line caso o resgate não seja pago (KLUSAITĖ, 2022); (5) *Spora*: Infecta o sistema através de phishing, agindo inicialmente como um usuário administrador, mostrando uma janela pop-up que não some até que o usuário a aceite (MESKAUSKAS, 2020); (6) *Petya*: Impede o acesso a todo o disco rígido, criptografando a tabela de arquivos mestre (BELCIC, 2019); (7) *Reveton*: Bloqueia as telas em vez de criptografar os arquivos (LESSING, 2020); (8) *Cerber e Locky*: Pesquisam e criptografam tipos específicos de arquivos, geralmente documentos e arquivos de mídia (AVAST, 2020). Dependendo da forma de ataque e os arquivos infectados é possível identificar o tipo de *Ransomware* (SILVA; GLÓRIA JÚNIOR, 2023).

O *Ransomware* pode acarretar diversos impactos há uma empresa, os principais são perda de dados, interrupções dos negócios, demissões e até danos a sua reputação, o que pode afetar sua situação financeira e consequentemente a capacidade de manter os seus funcionários, acarretando corte de custos. Em alguns casos a demissão pode ocorrer por conta de uma certa culpa de um funcionário que foi enganado pelos criminosos e serviu como porta de entrada (BERTOLUCCI, 2019).

No ano de 2021, o Brasil ficou marcado por ataques a grandes empresas, que trouxeram a vista à problemática de Segurança da Informação, sendo uma delas as Lojas Renner, varejista do ramo de vestuários (PACETE, 2021).

O ataque à Renner foi um marco importante na segurança nacional porque suas implicações de longo alcance trouxeram a questão à tona (GAIDARGI, 2021). A empresa divulgou um comunicado explicando que sua infraestrutura de Tecnologia da Informação (TI) sofreu um ataque cibernético que interrompeu alguns sistemas e operações da empresa. Também enfatizou que agiu rapidamente e ativou os protocolos e procedimentos de segurança existentes para conter o ataque e mitigar o impacto potencial (UPX, 2021). A Lojas Renner destacou que utiliza tecnologias e padrões rígidos de segurança da informação e continua se aprimorando para melhorar cada vez mais os protocolos e sistemas de

privacidade em sua infraestrutura (GUIMARÃES, 2021).

2.3. Setor de Construção

O setor de construção civil é um setor chave, pela sua capacidade de gerar efeitos na produção, na renda e no emprego, o que torna essa atividade fundamental para o desenvolvimento econômico do país (CUNHA, 2012).

Os principais players que podem ser encontrados no mercado são a Votorantim, a Intercement, a Polimix e a Supermix (SOUZA, 2023). Em relação a Votorantim, é uma empresa com mais de 80 anos de história e que atua na área do cimento, agregados, argamassas, concreto, plastificante e aditivos, possui mais de 50 unidades por todo o Brasil (VOTORANTIM, 2023).

A Intercement é uma empresa que atua na área de cimento há mais de 50 anos, possuindo mais de 20 unidades em território nacional e internacional, como Moçambique, Argentina e África do Sul (INTERCEMENT, 2023).

Outra empresa do setor é a Polimix que atua na área do concreto, agregados, argamassas, concreto fino e transporte a granel há mais de 40 anos, possuindo mais de 200 unidades em território nacional e internacional (POLIMIX, 2023).

Há mais de 40 anos, a Supermix atua no setor de engenharia de concreto, realizando a mistura, transporte e lançamento de concreto usinado, contando com mais de 120 unidades espalhadas em todo território nacional (SUPERMIX, 2023).

O setor é regido, dentre diversos sindicatos, o Sindicato dos Trabalhadores e Empregados em Concreteiras e Empresas de Bombeamento e Locação de Bombas no Estado de São Paulo (Sindeconbesp) que é responsável por promover boas condições de trabalho, proteger os seus direitos e representar seus filiados judicialmente (EXAME, 2022).

3. Metodologia

A metodologia utilizada foi estudo de caso único (YIN, 2021), pois o estudo tem como objetivo, entender como o Plano de Continuidade de Negócios pode auxiliar diante a um ataque de *Ransomware*, com natureza de pesquisa qualitativa (THEOPHILO; MARTINS, 2016). A coleta dos dados (GIL, 2022) foi através de entrevistas e análises documentais. A unidade de análise foi a Empresa-Alpha. Na Tabela 1 são apresentadas as características utilizadas para realização do trabalho.

Tabela 1 - Características do estudo

Item	Descrição	Autor(es)
Questão de Pesquisa	"Como o Plano de Continuidade de Negócios pode contribuir para a restauração dos serviços em uma empresa do setor de construção após um ataque *Ransomware*?"	
Natureza	Qualitativa	Gil (2022)
Metodologia	Estudo de Caso Único	Yin (2021)
Coleta de Dados	Entrevista Análise Documental	Theóphilo; Martins (2016)
Unidade de análise	Departamento de tecnologia da informação da Empresa-Alpha	

3.1. Procedimentos Metodológicos

Conforme a Figura 1, as etapas desta pesquisa são:

Passo 1: Criar o questionário. Foi criado um questionário para o levantamento de dados a ser encaminhado aos funcionários-chaves baseado no referencial teórico (Tabela 2) com um total de 12 questões para serem aplicadas nos respondentes e reorganizada de acordo com a temporalidade e assuntos (Anexo A).

Tabela 2 - Base Teórica e Questões

Base Teórica	Questões
O PCN pode ser otimizado pelo uso de boas práticas (ISO, 2013), tais como *Information Technology Infrastructure Library* (ITIL, 2019), *Control Objectives for Information and Related Technologies* (COBIT, 2021), *Balanced Scorecard* (BSC, 2021) e *Business Impact Analysis* (BIA, 2023).	Quais as boas práticas que são utilizadas no PCN?
O *Ransomware* é um tipo de *malware* que sequestra os arquivos de um computador, exigindo um pagamento para liberá-los, em que por meio de técnicas de engenharia social, exploração de vulnerabilidades em sistemas operacionais e aplicativos (INSIDE, 2023), com propagação via e-*mails* de *phishing* e *download* de *software* maliciosos (SILVA; GLÓRIA JÚNIOR, 2023).	Como ocorreu o ataque de *Ransomware* na empresa? Qual foi a origem do ataque?
O PCN é um documento que mostra o que uma empresa deve fazer quando houver interrupções, ajudando a empresa a lidar com diferentes problemas que podem acontecer e diz o que fazer em cada situação (FONTES, 2017).	A empresa realizou quais procedimentos para responder ao ataque *Ransomware*?

Base Teórica	Questões
O *Ransomware* pode acarretar diversos impactos há uma empresa, os principais são perda de dados, interrupções dos negócios, demissões e até danos a sua reputação (BERTOLUCCI, 2019).	Quais os danos causados pelo incidente?
A Lojas Renner divulgou um comunicado explicando que sua infraestrutura de TI sofreu um ataque cibernético que interrompeu alguns sistemas e operações da empresa, ela enfatizou que agiu rapidamente e ativou os protocolos e procedimentos de segurança existentes para conter o ataque e mitigar o impacto potencial (Upx, 2021).	Como ficou a imagem da empresa na visão dos clientes? Como foi o processo de restauração total da rede?
A Lojas Renner destacou que utiliza tecnologias e padrões rígidos de segurança da informação e continua se aprimorando para melhorar cada vez mais os protocolos e sistemas de privacidade em sua infraestrutura (GUIMARÃES, 2021).	Quais as mudanças realizadas após o ocorrido?
O plano de continuidade de negócio deve ser desenvolvido tendo em conta as especificidades da empresa, focando-se nas suas reais necessidades para garantir a eficiência operacional e minimizar os custos financeiros, que visa atender aos requisitos dos processos, incluindo testes de contingências integrados com locais de negócios, fornecedores críticos e conexões externas para atingir os tempos de recuperação exigidos pela criticidade do negócio (ROSINI; NEUBARTH, 2023).	Quais os principais serviços críticos e o que é planejado para evitar a interrupção no desenvolvimento de PCN? Para você qual foi o papel do Plano de Continuidade de Negócios (PCN) na contingência do ataque *Ransomware*?
O PCN é um processo que busca garantir a resiliência de uma organização contra danos e interrupções, isso é alcançado por meio de uma estrutura estratégica e operacional adequada (WEILL; ROSS, 2020).	Quais mudanças preventivas foram feitas no PCN após o ataque? Em relação ao PCN, quais as mudanças foram feitas após o ataque?

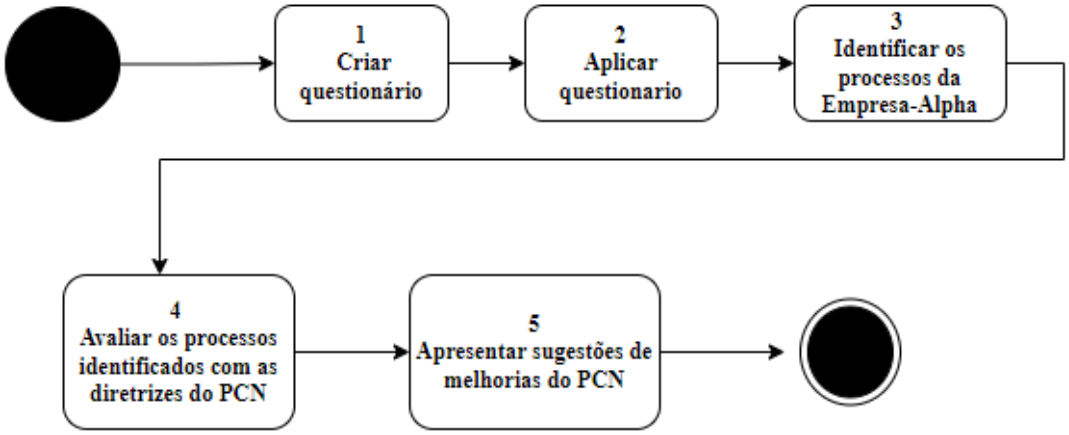
Passo 2: Aplicar o questionário. Foram entrevistados os responsáveis pela Empresa-Alpha seguindo o protocolo de entrevistas;

Passo 3: Identificar os processos da Empresa-Alpha. Foram levantados por meio de análise documental e entrevistas;

Passo 4: Avaliar os processos identificados com as diretrizes do PCN;

Passo 5: Apresentar sugestões de melhorias ao Plano de Continuidade de Negócios existente.

Figura 1 - Procedimentos Metodológicos



3.2. Objeto de Estudo

A Empresa Alpha é uma corporação que possui sua matriz no estado de São Paulo há mais de 20 anos, possui mais de 70 unidades espalhadas por todo o território brasileiro e internacionalmente, possuindo mais de 500 colaboradores espalhados por suas filiais.

Atualmente a empresa-alpha atua nas áreas de concreto, agregados, transporte a granel, também possui alguns projetos voltados para a área ambiental, como energia renovável e projeto de reciclagem de pneus.

Alguns dos principais projetos realizados pela Empresa-Alpha foram as obras da transposição do rio São Francisco e a obra do Rodoanel Mário Covas, um dos maiores projetos da empresa.

3.3. Perfil dos Respondentes

Foi realizado o piloto com o respondente 1 (R01) em 17/04/2024 em que conseguiu entender e responder as questões, desta forma, foi considerado o questionário validado. As demais entrevistas ocorreram de 22/04/2024 até 20/05/2024.

O perfil dos respondentes, como apresentado na Tabela 3, foi considerado aqueles que estão envolvidos diretamente com a área de TI ou possuem algum poder decisório na empresa.

Tabela 3 - Perfil dos Respondentes

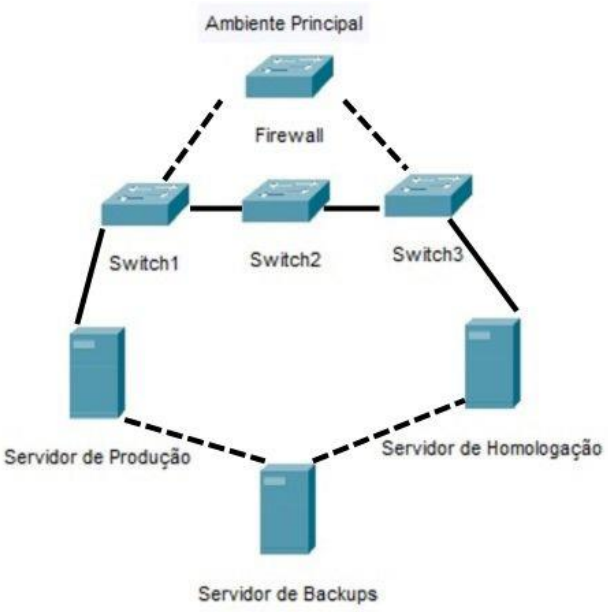
#	Responsabilidade	Tempo na área	Tempo na Empresa
R01	Analista	6 anos	7 anos
R02	Líder	6 anos	3 anos
R03	Líder	5 anos	2 anos
R04	Líder	5 anos	1 ano
R05	Líder	15 anos	4 anos
R06	Líder	11 anos	5 anos
R07	Analista	5 anos	5 anos
R08	Analista	6 anos	3 anos
R09	Analista	10 anos	10 anos

4. Resultados e Discussões

4.1. Identificação da estrutura da Empresa-Alpha

A estrutura tecnológica da empresa é dividida por um ambiente principal (Figura 2) e um ambiente de replicação, que atua se algum equipamento do ambiente principal parar de funcionar.

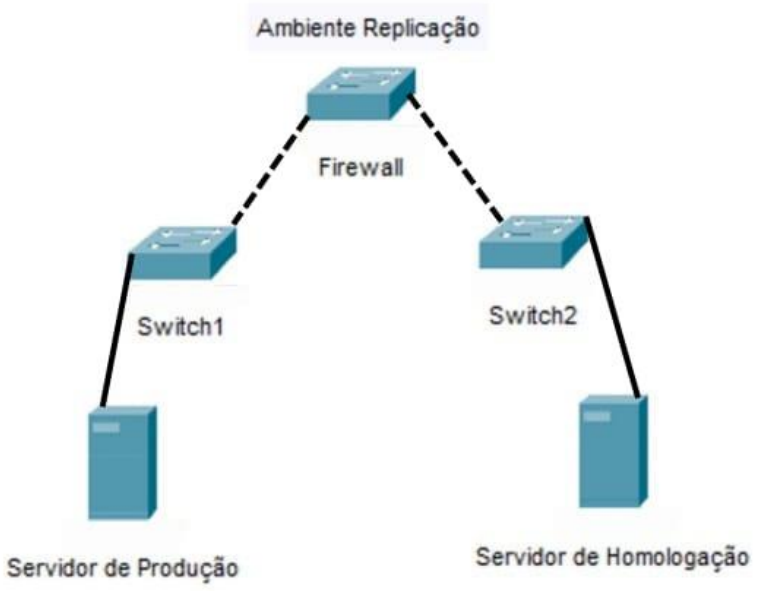
Figura 2 - Ambiente Principal



No ambiente principal a Empresa-Alpha possui um *firewall* que realiza a proteção da rede, *switches* que enviam internet para os servidores, *acess points* e para as mesas dos integrantes. Existe um servidor NAS (*Network Attached Storage*) que realiza os *backups* localmente e também é feito pela nuvem, utilizando o Microsoft Azure.

O ambiente de replicação (Figura 3), possui basicamente a mesma estrutura do ambiente principal, mudando apenas a quantidade de *switches* e não existe o servidor de *backup*, pois os *backups* da replicação são feitos pelo Microsoft Azure.

Figura 3 - Ambiente Replicação



4.2. Histórico do Ataque Sofrido na Empresa-Alpha

O ataque ocorreu em pela manhã do dia 06 de abril de 2021, o qual foi identificado após alguns integrantes informarem que não estavam conseguindo acessar as pastas de seus respectivos departamentos, conforme relatos de R01, R03 e R4.

A origem do ataque foi através de um IP estrangeiro que, após ser identificado, foi bloqueado pela equipe, segundo afirmou R09: "...se tratava de um IP fora do Brasil...". O R01 sugere que o atacante pode ter conseguido acesso as credenciais de um integrante da Empresa-Alpha mediante a um ataque phishing, conforme informa em: “...o atacante tinha conseguido as credenciais de acesso de um integrante da TI provavelmente por conta de *phishing*...”.

O principal dano causado pelo ataque foi o atraso nas demandas, atrasando pagamentos, entrega de relatórios e multas, já que o servidor afetado foi o *file server* que continha as principais planilhas, documentos importantes e contratos.

Não foi necessário o pagamento ao atacante graças a rotina de *backups* e replicações que a Empresa-Alpha possuía, conforme R01: "...graças as rotinas de *backups* e replicações a empresa conseguiu realizar a restauração dos arquivos sem a necessidade de pagamento ao atacante..." e R02: "... após isso nossos acessos foram aos poucos sendo restaurados....", levando cerca de três dias para restauração total dos departamentos, na restauração foi dado prioridade aos departamentos que tinham mais urgência.

Neste período de restauração foi realizado o bloqueio do IP, algumas mudanças nas permissões de acesso dos integrantes, segundo afirmou R08: "... foi identificado o IP e bloqueado no *firewall* via GEO-IP, realizamos mudanças nas permissões de acesso dos integrantes..." e identificado a máquina pelo qual o atacante conseguiu acesso aos arquivos, conforme R01: "...identificamos a máquina que apresentou a vulnerabilidade e desativamos o usuário que nela se encontrava...".

4.3. Sugestões de Mitigação

As sugestões, conforme Tabela 4, foram consideradas com a intenção de mitigar as vulnerabilidades encontradas e prevenir que o ataque ocorra novamente.

Tabela 4 - Vulnerabilidades versus Ações

#	Vulnerabilidade	Ações Empresa-Alpha	Ações Sugeridas
1	Senha fraca	Revisão de senhas	Política de senha fortes, utilização do MFA (Multifator de Autenticação)
2	Permissões de acesso	Revisão de permissões	Restringir permissões por necessidades
3	Backups inadequados	Backups diários e testes de recuperação	Backups regulares de seus arquivos mais importantes de forma automática
4	Falta de conhecimento	Treinamento	Treinamentos e palestras de conscientização contra *Ransoware*
5	Plano de Continuidade de Negócios incompleto	Atualização do PCN	Desenvolver, implementar e testar o PCN

4.4. Sugestões de Melhoria do PCN

Após o ataque, a Empresa-Alpha realizou algumas mudanças em seu Plano de Continuidade, conforme a Tabela 5, foram sugeridas mais duas mudanças para a Empresa-Alpha.

Tabela 5 - Mudanças no PCN

#	Mudanças Empresa-Alpha	Mudanças Sugeridas
1	Revisão constante do Plano de Continuidade de Negócios	Atualização regular e revisões do PCN
2	Documentações detalhadas	Plano de Contingência detalhado
3	Análise dos riscos	Avaliação de riscos atualizada
4	Não houve ações	Comunicação eficaz
5	Não houve ações	Relatórios e auditorias

5. Considerações Finais

Em conclusão, um plano de continuidade de negócios é essencial para a sobrevivência e o sucesso de uma organização diante de eventos imprevistos ou crises. Graças ao PCN a Empresa-Alpha conseguiu passar pelo ataque sem maiores danos, pois possuía uma rotina de *backups* que ajudou a restaurar seu ambiente sem a necessidade de pagamento ao atacante.

Os principais resultados indicaram que o Plano de Continuidade de Negócios é extremamente importante para diversos tipos de empresas, incluindo as dos setores de construção. Com a adoção das boas práticas do PCN, a Empresa-Alpha conseguiu identificar os serviços críticos e mitigar as vulnerabilidades encontradas em seu sistema.

A contribuição prática foca em fornecer sugestões de melhoria e de mitigação sobre o Plano de Continuidade de Negócios, permitindo que os gestores as incorporem em suas empresas. As contribuições teóricas destacam a importância do plano de continuidade de negócios em relação à um ataque de *Ransomware*.

Referências

AVAST. *Ransomware* Cerber: Tudo que você precisa saber. 2020.

BELCIC, I. *Ransomware* Petya: Como funciona e como se proteger. 2019.

BERTOLUCCI, G. *Ransomware* causa demissão de 300 funcionários de empresa, MG. 2019.

BIA. BIA - Business Impact Analysis. 2023.

BSC. BSC - Balanced Scoreboard. 2021.

BURDOVA, C. What Is Eternal Blue and Why Is the MS17-010 Exploit Still Relevant? 2022.

COBIT. COBIT - Control Objectives for Information and Related Technologies. 2021.

CUNHA, G. DE C. A importância do setor de construção civil para o desenvolvimento da economia brasileira e as alternativas complementares para o Funding do crédito imobiliário no Brasil. 2012.

EXAME. O que é sindicato e como ele funciona. 2022.

FONTES, E. L. G. **Segurança da Informação**. SP: Saraiva Educação SA, 2017.

GAIDARGI, J. **RENNER É VÍTIMA DE *RANSOMWARE* – E SE FOSSE VOCÊ?** Disponível em: <https://infonova.com.br/renner-ransonware-consequencias-solucoes/>.

GIL, A. C. **Como elaborar projetos de pesquisa**. 7. ed. [s.l.] Atlas, 2022.

GUIMARÃES, L. **Site da Renner sai do ar após ataque hacker – entenda o caso**. Disponível em: <https://www.cnnbrasil.com.br/economia/site-da-renner-continua-fora-do-ar-apos-ataque-hacker/>.

INSIDE, T. Setor Financeiro é o segundo mais atingido por ataque de *Ransomware*s. 2023.

INTERCEMENT. Disponível em: <https://brasil.intercement.com>.

ISO. ISO 22301 - Societal security – Business continuity management systems. 2013.

ITIL. ITIL - Information Technology Infrastructure Library. 2019.

KLUSAITĖ, L. *Ransomware*: o que é e como se proteger? 2022.

LESSING, M. Case Study: Reveton *Ransomware*. 2020.

MARION, N. E.; TWEDE, J. **Cybercrime: an encyclopedia of digital crime**. 1. ed. USA: Bloomsbury Publising USA, 2020. v. 1

MESKAUSKAS, T. *Ransomware* Spora. 2020.

MOURA, B. *Ransomware* Locker: o que é e como evitar. 2022.

PACETE, L. G. **5 ataques cibernéticos no Brasil em 2021 que geraram alerta**. Disponível em: <https://forbes.com.br/forbes-tech/2021/12/5-ataques-ciberneticos-no-brasil-em-2021-que-geraram-alerta/>.

POLIMIX. Disponível em: <https://www.polimix.com.br/index.html>.

RAMOS, G. O que é scareware? Entenda o programa malicioso que “causa medo”. 2021.

ROSINI, A. M.; NEUBARTH, R. H. Governança corporativa e a gestão de continuidade de negócios: estudo de caso múltiplo em empresas do setor financeiro brasileiro. **Refas-Revista Fatec Zona Sul**, v. 9, n. 5, p. 1–23, 2023.

SILVA, S.; GLÓRIA JÚNIOR, I. *Ransomware*: A Evolução Dos Ataques Na Contemporaneidade e Seus Desafios para a Segurança Digital. **Journal of Technology & Information (JTnI)**, v. 3, n. 2, 2023.

SOUZA, N. **9 maiores fábricas de cimento do Brasil**. Disponível em: <https://sohelices.com.br/9-maiores-fabricas-de-cimento-do-brasil/>.

SUPERMIX. Disponível em: <https://www.supermix.com.br>.

THEOPHILO, C.; MARTINS, G. DE A. **Metodologia Da Investigação Cientifica**. [s.l.] Atlas, 2016.

UPX. ***Ransomware*: entenda o caso que abalou a Renner e conheça os diferentes tipos de ciberataques.** Disponível em: <https://upx.com/post/*Ransomware*-renner/>.

VOTORANTIM. Disponível em: <https://www.votorantimcimentos.com.br>.

WEILL, P.; ROSS, J. W. **Governança de TI: como as empresas com melhor desempenho administram os direitos decisórios de TI na busca por resultados superiores**. Brasil: M. Books, 2020. v. 1

YIN, R. K. **Case Study Research and Applications: Design and Methods**. 6. ed. [s.l.] Sage Publications, Inc., 2021.

Anexo A – Questionário

Conteúdo: Ataque de *Ransomware*

#	Pergunta
Q01	Como ocorreu o ataque de *Ransomware* na empresa?
Q02	Qual foi a origem do ataque?
Q03	A empresa realizou quais procedimentos para responder ao ataque *Ransomware*?
Q04	Quais os danos causados pelo incidente?

Conteúdo: Pós Ataque de *Ransomware*

#	Pergunta
Q05	Como foi o processo de restauração total da rede?
Q06	Quais as mudanças realizadas após o ocorrido?
Q07	Em relação ao PCN, quais as mudanças foram feitas após o ataque?
Q08	Quais medidas preventivas foram criadas por meio do PCN?
Q09	Como ficou a imagem da empresa na visão dos clientes?

Conteúdo: Plano de Continuidade Negócios, após o ataque de *Ransomware*

#	Pergunta
Q10	**Quais as boas práticas que são utilizadas no PCN?**
Q11	**Quais os principais serviços críticos e o que é planejado para evitar a interrupção no desenvolvimento de PCN?**
Q12	**Para você qual foi a importância do Plano de Continuidade de Negócios na contingência do ataque *Ransomware*?**

Anexo B – Protocolo de Entrevista

O protocolo de entrevista aplicado aos respondentes possui os seguintes passos:

- **Passo 1.** Realizar a introdução sobre o pesquisador e a pesquisa a ser feita;
- **Passo 2.** Descrever como será conduzida a entrevista;
- **Passo 3.** Ressaltar a preocupação da confidencialidade e privacidade dos entrevistados. Explicar como os dados coletados serão mantidos no anonimato;
- **Passo 4.** Iniciar as questões (Anexo A);
- **Passo 5.** Perguntar se há alguma outra observação que seria interessante para a pesquisa;
- **Passo 6.** Finalizar a entrevista.