Lab de Tendências I Casa Firjan

RISCOS CIBERNÉTICOS NAS EMPRESAS

51º Dossiê

15/06/2021

SOBRE O **LAB DE TENDÊNCIAS**

quem somos?

Como forma de pensarmos juntos sobre **futuros possíveis** a partir das mudanças do cenário atual, estamos produzindo dossiês com conteúdos pertinentes a esse contexto.

O objetivo do material é compartilhar **boas práticas** e **oportunidades de ação** em prol da manutenção do ecossistema empresarial e sua relação positiva com a sociedade.

O Lab de Tendências da Casa Firjan pensa cenários futuros de transformação que irão impactar as empresas e os profissionais.

RISCOS CIBERNÉTICOS NAS EMPRESAS

A partir das discussões sobre os **ataques e ameaças cibernéticas que afetam as empresas e as respostas possíveis a eles,** fomentadas pelo Aquário Casa Firjan, série de palestras e debates semanais, ocorrido no dia 15/06/2021, vamos analisar como os riscos e ameaças do ambiente digital atingem as empresas e quais práticas de segurança podem ser aplicadas.

CONTEXTO **ATUAL**

Panorama Atual

- Desde 2020 vem ocorrendo um aumento alarmante no número de ameaças e ataques cibernéticos pelo mundo, seja contra empresas, governos ou indivíduos;
- Estes ataques atingem **ambientes virtuais** para **captação ou danificação de dados e informações**, podendo causar, inclusive, prejuízos financeiros ao negócio;
- O crescente uso de **tecnologias emergentes**, como aprendizado de máquina, inteligência artificial e 5G, pelos hackers tem tornado mais complexa a implementação de práticas de segurança eficazes contra estas ameaças.

Panorama Brasil

- O Brasil foi o país da América Latina que mais sofreu **ataques cibernéticos** no ano de 2020;
- Até o terceiro trimestre do ano passado foram registrados 3,4 bilhões de tentativas de ciberataques;
- O uso de softwares desatualizados é uma das principais causas de ataque;
- A Lei Geral de Proteção de Dados Pessoais recentemente implementada busca contribuir para a **prevenção, o monitoramento e a resposta** ás ameaças e ataques cibernéticos..

CONCEITOS **FUNDAMENTAIS**

Conceito | Segurança da informação

A Segurança da informação busca **tratar e proteger os dados presentes em ambientes físicos e digitais**. Projetada para manter a **confidencialidade, integridade e disponibilidade** de dados, ela engloba Segurança Cibernética, Segurança Física, Segurança de TI e Segurança de Pessoas. Todas elas devem ser observadas pelas empresas para que seja feita a proteção contra acessos não autorizados a dados e informações presentes em sistemas computadorizados.

Conceito | Cibersegurança

Segurança cibernética ou cibersegurança é a área da Segurança da informação que atua no ambiente digital, tratando da prevenção, mitigação e recuperação frente às **ameaças e ataques cibernéticos**. Ela aponta práticas que buscam **proteger sistemas e ativos de informação ligados á internet**, como computadores, servidores, dispositivos móveis, redes e sistemas eletrônicos.

AMEAÇAS **MAIS COMUNS**

Vírus

Programa que, uma vez executado, pode ***danificar o computador, corromper e roubar dados***.

Ransomware

Software que ***codifica os dados do sistema e bloqueia o acesso dos usuários.*** *É* utilizado para ***sequestro.***

Phishing

Técnica que usa ***fraude, truque ou engano*** para manipular as pessoas e obter ***dados confidenciais.***

Spyware

Software que funciona em segundo plano ***coletando dados*** ou fornecendo ***acesso remoto ao hacker.***

BOAS PRÁTICAS **EM DESTAQUE**

Cultura consolidada

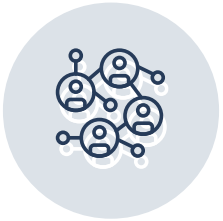
Criar uma cultura de cibersegurança, desenvolvendo políticas preventivas e códigos de conduta para colaboradores seguros.

Monitoramento

Manter uma rotina de monitoramento dos sistemas e redes contra ameaças conhecidas e desconhecidas.

Ação proativa

Ter respostas assertivas, eficazes e rápidas para as ameaças e ataques.



Redes de colaboração

Colaborar com outras empresas para aumentar o conhecimento sobre as ameaças e a capacidade de resposta a elas.

Máquinas corporativas seguras

Ter sistemas de segurança cibernética atualizados para as máquinas corporativas, permitindo monitoramento dos acessos, transações e ameaças.

TECNOLOGIAS DE **SEGURANÇA**

01.

VPN

A sigla significa **Rede Virtual Privada**, do inglês *Virtual Private Network*. É uma ferramenta que permite o acesso remoto seguro à rede da empresa. Ela cria um canal que diminui a vulnerabilidade das **transações remotas** de dados e informações.

02.

AUTENTICAÇÃO

A **dupla autenticação ou autenticação de dois fatores** é um mecanismo de **verificação do usuário**. Para acessar um ambiente virtual ou informação é exigido **duas formas de checagem**, como por exemplo, senha e código de acesso enviado por SMS.

03.

ANTIVÍRUS

É um **software** que protege o computador **contra ataques de programas maliciosos**, os chamados vírus. O antivírus deve ser instalado. Ele executa **varreduras frequentes** no computador para identificação de ameaças.

O QUE ESPERAR DO **FUTURO**

O desenvolvimento cada vez mais veloz de **novas tecnologias** e o aumento da **automação das atividades e processos** das empresas, alertam para o constante surgimento de novas ameaças cibernéticas. Frente a isso, o Fórum Econômico Mundial apontou 5 **desafios emergentes** para a segurança dos ecossistemas digitais que demandam ações conjuntas.

Aumento da **lacuna de habilidades** de segurança cibernética;

Fragmentação das abordagens técnicas e políticas para o tema;

Insuficiência das **capacidades operacionais e tecnologias** atuais;

Tecnologias **desenvolvidas sem considerar ameaças maliciosas.**

Falta de clareza para definir os **responsáveis por garantir** a segurança.

DESAFIOS

Uso da tecnologia

- Empresas que **não contam com uma área de Tecnologia da Informação** podem ter maiores dificuldades para identificar todas as vulnerabilidades e soluções possíveis em cibersegurança;
- Para lidar com as ameaças do ambiente virtual, as empresas podem contar com **serviços especializados** em segurança de dados como alternativa eficaz para se prevenir dos riscos cibernéticos.

Cultura organizacional

- Para que ciberataques sejam evitados é necessário a implementação de tecnologias adequadas ao modelo de negócios das empresas, assim como a **mudança de mentalidade e a adoção de hábitos seguros** no dia-a-dia das corporações;
- Os colaboradores precisam estar **conscientes e proativos frente aos perigos** que as interações e transações de dados e informações podem trazer.

OPORTUNIDADES

Novos segmentos

- O mercado **de produtos de segurança cibernética personalizados** é promissor para abertura de novos negócios;
- A quantidade de dados e informações sigilosos nas redes vem aumentando com a automação de processos e atividades de rotina de empresas e instituições;
- Personalizar sistemas de segurança pode **aumentar o grau de eficácia** das medidas tomadas.

Gerenciamento dos dados

- Ter consciência de quais dados e informações são gerados e utilizados pela empresa são um diferencial na adoção de medidas de segurança cibernética;
- A elaboração de uma política de cibersegurança pode ser um estímulo para que seja feita a **classificação dos dados e informações** da corporação;
- Esta organização dos dados de forma transparente permitirá ações que priorizem os ativos que são mais **relevantes e sensíveis** para os negócios.

REFERÊNCIAS

YouTube – Canal Firjan
Cibersegurança em xeque: Como as empresas devem agir para se proteger? | Aquário Casa Firjan

Participantes dos debates
Marco DeMello | CEO e cofundador da PSafe e Presidente do Grupo CyberLabs
Alfred Bacon | Presidente e fundador da ISACA
Vanessa Padua | Diretora de negócios em nuvem e cibersegurança da Microsoft

Mediação
Ana Cristina Carvalho | Gerente Geral de TI da Firjan

REFERÊNCIAS

https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-------what-you-need-to-know-for-2021/?sh=6f7914958d3d
https://www.weforum.org/platforms/the-centre-for-cybersecurity
https://www.weforum.org/agenda/2020/01/what-are-the-cybersecurity-trends-for-2020/
http://www3.weforum.org/docs/WEF_Future_Series_Cybersecurity_emerging_technology_and_systemic_risk_2020.pdf
http://midias.cebri.org/arquivo/Policy%20papers%20-%20XVI%20Forte%20Copacabana%202019%20-%20International%20Security%20Conference.pdf
https://www.nsctotal.com.br/noticias/o-guia-de-ciberseguranca-do-forum-economico-mundial
https://www.portaldaindustria.com.br/industria-de-a-z/ciberseguranca/
https://www.cobracorps.com.br/o-que-e-seguranca-cibernetica-cyber-security/
https://blog.starti.com.br/tudo-sobre-seguranca-cibernetica/
https://www.avast.com/pt-br/c-phishing
https://www.serpro.gov.br/lgpd

REFERÊNCIAS

citadas no debate

Relatório da Microsoft
Relatório de Defesa Digital da Microsoft | Setembro de 2020

Relatório da Gartner
Rethink Your Security & Risk Strategy: Gartner Cybersecurity 2021

Normas ABNT ISO/IEC
ISO/IEC 27001: Requerimentos para gestão de dados e segurança | 2013
ISO/IEC 27002: Boas práticas de segurança de dados | 2013
ISO/IEC 27701: Técnicas de segurança; Extensão das ISO/IEC 207001 e 27002 | 2019

TED
Ralph Langner: Decifrando o Stuxnet, uma arma do século XXI | 2019

QUER SABER MAIS?

referências complementares

Aquário Casa Firjan – 1h53min:
COVID-19: Como fica a cibersegurança das empresas com o trabalho remoto?

Artigo da plataforma digital Casa Firjan - 3 min (leitura)
O impacto da Covid-19 na segurança de dados das empresas | de Tatiana Fleming

Evento promovido pelo Senai– 1h01min:
Cibersegurança – A nova era dos dados

Podcast da MIT Technology Review Brasil - 34 minutos:
A inserção da cibersegurança na cultura corporativa | c/ Andre Miceli, Carlos Aros e Rafael Coimbra


Firjan IEL