BARRICADAS ESTRATÉGIAS E COLETIVIDADE

Uma cartilha de segurança digital para organizações

ÍNDICE

INTRODUÇÃO

Nossas relações pessoais e profissionais estão apoiadas em estruturas digitais que armazenam dados importantes e sensíveis. Por isso, o tema da Segurança da Informação tem aparecido com mais frequência em nosso cotidiano. Quando falamos sobre a segurança organizacional estamos nos referindo a protocolos, acordos e medidas que servem para aumentar a proteção da missão, da integridade da informação e da equipe de uma organização, movimento ou coletivo.

Esse tema é particularmente relevante quando falamos de instituições que trabalham na luta por direitos porque suas ações encontram muitos desafios quando confrontam estruturas de poder de repressão e de vigilância.

No último ano, acompanhamos diversos casos de ataques digitais contra organizações, coletivos e movimentos sociais. Esses ataques podem ter sido motivados por causas políticas ou podem ter sido produto de vulnerabilidades exploradas por pessoas mal intencionadas. O fato é que causaram impactos significativos nessas organizações.

Quando as organizações buscam apoio para melhorar suas práticas de segurança, normalmente se deparam com consultorias especializadas em Tecnologia da Informação e profissionais que falam um linguajar técnico e distante do entendimento da equipe.

Consideramos importante que o conhecimento para a segurança organizacional seja mais acessível e didático e que os relatos de casos reais ajudem a sensibilizar sobre o tema.

Este material está dividido em duas partes. Começamos com uma análise do impacto de ataques digitais do tipo 'Ransomware' em organizações brasileiras. Depois abordamos a segurança organizacional em tópicos, trazendo recomendações para apoiar na adoção de protocolos e boas práticas.

Por que discutir segurança digital com a sociedade civil?

No final de 2018 registramos ameaças às organizações da sociedade civil brasileiras, em especial àquelas que atuam na defesa de direitos humanos. Assim, atendendo ao pedido de apoio das parceiras no Brasil, a **Pão para o Mundo (PPM)** decidiu promover uma formação durante o ano de 2019. Os principais objetivos foram:

I) *a sensibilização sobre aspectos gerais e holísticos ao redor da segurança digital;*

II) *o aumento da compreensão sobre segurança das equipes por meio de práticas, táticas e uso de ferramentas estratégicas;*

III) *apoio ao desenvolvimento de habilidades e boas práticas em segurança digital, incluindo as ferramentas para comunicação, considerando riscos, alternativas e opções.*

As oficinas foram organizadas pelo **ELO Ligação e Organização** e desenvolvidas pela coletiva **Marialab**, com dois dias de duração e distribuição de material para compartilhamento com as equipes de trabalho. Ao longo de 2019, foram realizadas seis oficinas presenciais, nas cidades de São Paulo/SP, Rio

de Janeiro/RJ, Belém/PA, Recife/PE, Porto Alegre/RS e Brasília/DF, com participação de 56 organizações e 103 pessoas.

Concluída esta primeira etapa, oferecemos agora esta cartilha, que tem por objetivo dar continuidade ao processo de sensibilização e informação sobre os riscos existentes. Incluímos as ações recomendadas para proteção das organizações e suas equipes de trabalho, em especial nos casos de ataques e sequestro dos dados e arquivos institucionais.

Esperamos que o material seja amplamente divulgado para as pequenas, médias e grandes organizações da sociedade civil, contribuindo para o direto à livre associação e atuação para a construção de um mundo com maior justiça e inclusão social.

PARTE 1

RANSOMWARE

O sequestro de dados e como ele ameaça as organizações de luta por direitos

Dentre os diversos tipos de ameaças digitais, o Ransomware é um malware que pode afetar severamente o dia a dia de uma organização. Esse programa malicioso infecta computadores e bloqueia o acesso aos arquivos, exigindo um pagamento em **bitcoins** como resgate. Em inglês, a palavra "ransom" quer dizer resgate.

O Ransomware é uma ameaça global que afeta em grande parte computadores com Windows[1]. Sua distribuição acontece principalmente através de links em e-mails falsos (**phishing**) ou explorando brechas de segurança em servidores mal configurados. Há diversas famílias de Ransomware.

Em 2019, os ataques realizados por meio dessa ameaça digital cresceram 118% em relação a 2018[2] e nada indica que isso vá desaparecer ou diminuir no futuro.

Mesmo sendo uma ameaça cujo principal alvo são grandes empresas (81% em 2018), o Ransomware também infecta agências do governo, hospitais, escolas e organizações do terceiro setor[3].

Desde 2017, algumas organizações brasileiras que lutam por direitos foram vítimas desse malware, e isso aumentou em 2019. Entrevistamos as organizações atacadas para entender o impacto dessa ameaça em suas atividades. Vamos contar essas experiências para que outros grupos semelhantes possam aprender a se prevenir a partir desses relatos.

1 - Um ataque de ransomware em etapas

João voltou ao trabalho após as férias de Carnaval. Ligou seu computador e foi pegar um café na copa. Voltando para sua mesa, notou algumas pessoas cochichando assustadas em volta dos computadores. Assim que tentou acessar a internet recebeu uma mensagem muito estranha em inglês, independente do site que tentava acessar. Cinco minutos depois, uma pessoa da equipe de TI apareceu e pediu para todos desligarem os computadores, pois teriam de ser formatados um a um.

1 - https://www.statista.com/statistics/701020/major-operating-systems-targeted-by-ransomware/

2 - https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf

3 - https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/

1.1- Como era a situação das organizações em relação a segurança digital antes do ataque

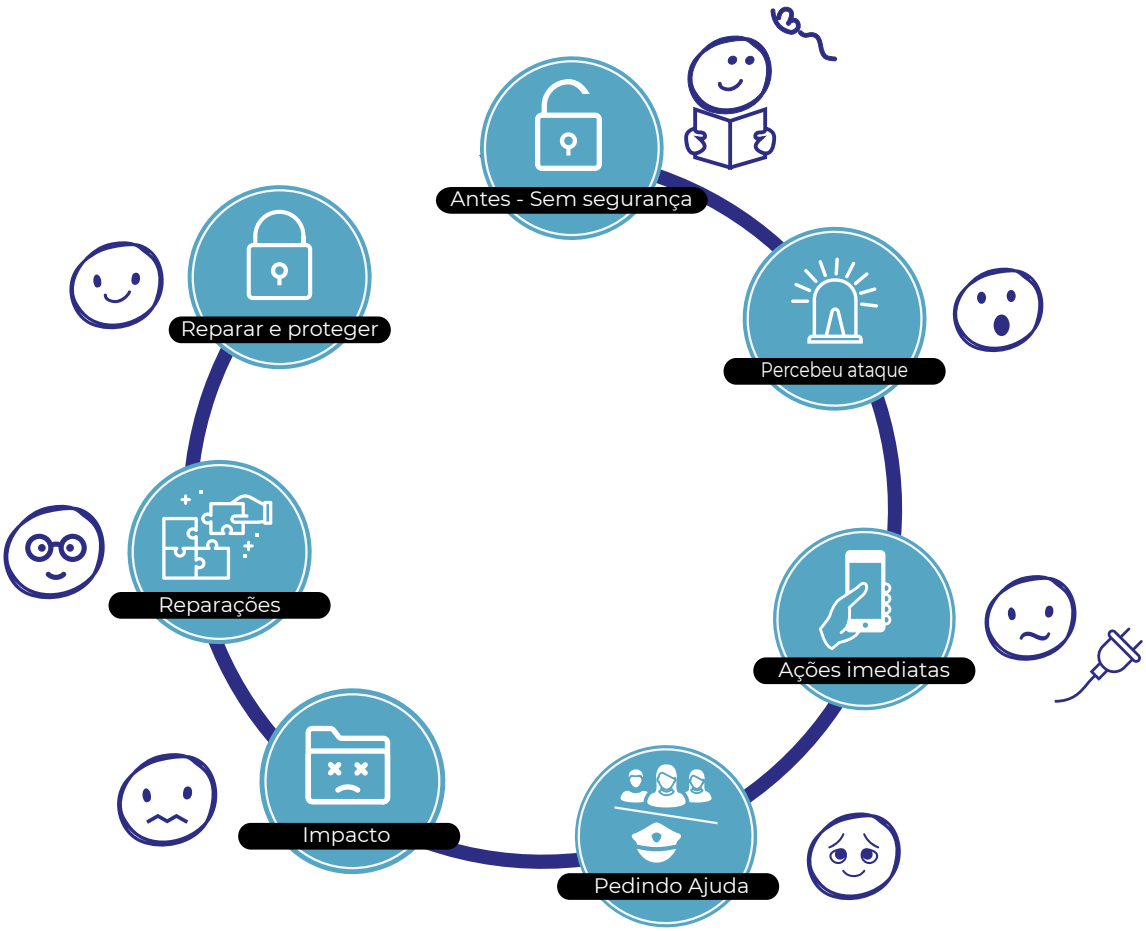
Podemos dizer que todas as organizações já tinham algum tipo de contato com o tema da segurança física, pois os contextos de seu trabalho exigem uma atenção forte a esse tema. Contudo as ameaças digitais ainda pareciam muito distantes e com impactos desconhecidos.

A maioria das equipes tinham profissionais de Tecnologia da Informação (TI) contratados, mas esses não eram especialistas em segurança digital e não tinham experiência prévia com esse tipo de ataque.

Antes dos ataques as organizações entrevistadas tinham total confiança nesses técnicos e pouco controle de suas ações. A responsabilidade da segurança digital ficava quase completamente nas mãos dessas pessoas.

Identificamos que existiam práticas fracas de segurança de senha e backup e que apesar de em alguns casos essas vulnerabilidades terem sido identificadas antes do ataque, as medidas de correção eram lentas e ainda estavam em implementação.

Outra coisa comum entre as organizações é que não esperavam que algumas áreas como financeiro e administrativo fossem potenciais alvos, já que eram setores que não tinham visibilidade para o público externo.



1.2 – Como o ataque foi percebido dentro da organização

Nenhuma das organizações esperava algum ataque digital, pois estavam envolvidas com suas agendas, saindo de recessos e planejamentos. Na maioria dos casos os profissionais de TI foram as primeiras pessoas a notar que algo estava acontecendo, mas não identificaram imediatamente a natureza do ataque, seu tamanho e seus impactos.

Após a detecção as organizações pararam seus trabalhos parcialmente ou completamente, e devido a falta de informação houve uma demora para comunicar a equipe do ocorrido, o que causou estresse e tensões entre as pessoas. Também houve muita insegurança sobre a tomada de decisões porque eram casos inéditos. Isso adicionou outro grau de estresse ao lidar com as situações.

Praticamente nenhuma organização identificou como foi atacada, mas a maioria das evidências apontam para brechas no servidor e para download de anexos de e-mail com vírus.

1.3 – Quais foram as ações imediatas

Ao perceber os ataques, a maioria das pessoas que estavam analisando o fato tomaram a decisão de desconectar as máquinas da rede e da internet. Isso foi decisivo para duas organizações: uma conseguiu impedir que o ataque se espalhasse por toda a infraestrutura do escritório e outra conseguiu impedir que o vírus afetasse os arquivos de backup.

Em alguns casos não se soube como proceder ou foram tomadas medidas imediatas que impactaram muito a equipe, como impedir o acesso aos computadores ou formatá-los sem realizar backup, porque acreditavam que os arquivos estariam saudáveis no servidor. Não estavam.

A contratação de especialistas e busca de ajuda na rede de apoio foi essencial para mitigar o ataque nesses primeiros momentos.

1.4 – Como aconteceu a busca de ajuda

A busca imediata de ajuda foi a pessoas consultoras técnicas conhecidas pela rede das organizações, ou profissionais do mercado. Em todas as entrevistas foi relatada a busca de ajuda de organizações parceiras que já haviam sido atacadas de forma semelhante.

Em quase todos os casos se fez denúncias nas delegacias de crimes cibernéticos ou equivalentes em suas cidades, mas não se recebeu respostas positivas e maiores orientações. Apesar disso todos relataram a importância do Boletim de Ocorrência para buscar apoios financeiros e comprovar a ocorrência do ataque.

Nenhuma organização conseguiu encaminhar os casos para investigações forenses. Nenhuma recebeu apoio financeiro específico para reestabelecer sua infraestrutura, tendo de utilizar dinheiro de caixa próprio ou readequar rubrica de projetos em aberto.

Grande parte das organizações relatou que depois de comunicar o ocorrido à equipe, houve momentos de tristeza e estresse, mas que ao final as pessoas se uniram para recuperar seus trabalhos e superar o fato.

1.5 – Qual foi o impacto do ataque

Todas as organizações entrevistadas relataram impactos significativos em sua rotina de trabalho, na sua percepção de segurança, no nível de estresse da equipe e em gastos não antecipados em seus planejamentos institucionais. Também houve atrasos em prestação de contas e em renovações de contratos com instituições financiadoras.

Foi relatada a perda de arquivos de dezenas de anos de trabalho. Os departamentos mais impactados foram o financeiro e administrativo, porém o impacto foi percebido em toda a organização, variando entre atrapalhar alguns dias de trabalho a seis meses.

Os gastos financeiros incluíram itens como compra de novos equipamentos, muitas horas de trabalho para refazer ou reencontrar arquivos, novas contratações de técnicos e serviços, negociações com os atacantes, nova instalação de redes, entre outros.

1.6 – O que foi feito após o ataque

Houve tentativas de recuperar os arquivos criptografados por meio do pagamento de resgate ou da contratação de especialistas, mas nenhuma delas foi bem sucedida.

As organizações que tinham algum tipo de backup dos arquivos recorreram a esses para recuperar suas informações. Algumas tinham arquivos em papel, usados para reconstruir seus dados digitais.

Todas as organizações tomaram alguma medida para aumentar a segurança digital. A maioria delas teve que adquirir novos servidores internos e reinstalar sistemas.

Muitas organizações optaram por buscar um novo profissional de TI, na busca por serviços que respondessem melhor suas demandas. Algumas buscaram manter uma aproximação com coletivos e grupos parceiros que proveram ajuda com o Ransomware, estabelecendo uma relação complementar, além da pessoa contratada para as demandas corriqueiras de TI.

1.7 – O que mudou na organização

O acontecimento forçou a implementação rápida de medidas de backups e segurança de servidores e trouxe à tona a importância do tema nas políticas institucionais. Futuras instalações de ferramentas de segurança, protocolos e treinamentos da equipe foram planejados.

Os relatos nos revelam, entretanto, que apesar de entender a prioridade do tema, ainda é muito difícil para as organizações inserirem práticas de segurança em seu dia a dia. As principais dificuldades relatadas foram estabelecer horas de trabalho específicas para o treinamento da equipe, encontrar recursos financeiros para recompor a infraestrutura digital, elaborar políticas de segurança e manter uma agenda de aprendizagem sobre o assunto.

1.8 – Conclusões e recomendações

Entendemos que uma política de segurança poderia ter ajudado na tomada de decisões antes, durante e após os ataques. Alguns protocolos de segurança ajudariam a diminuir as vulnerabilidades exploradas pelo malware e a garantir menor perda de informação. Uma orientação de como a equipe poderia proceder em casos de emergência digital seria útil para diminuir a ansiedade relatada.

Percebemos que o fato de deixar nas mãos dos profissionais de TI todas as medidas de segurança deixou as organizações mais vulneráveis, porque existia pouco controle sobre as implementações de proteção da infraestrutura digital e poucas práticas de comportamento seguro da equipe. No momento de crise, poucas pessoas sabiam como agir e quase todas as pessoas entrevistadas relataram incerteza em relação às medidas que foram tomadas para conter o Ransomware.

1.9 - Como se defender

Um computador está com os arquivos inacessíveis e em todas as pastas há um arquivo de texto com a mensagem: 'Os seus arquivos foram criptografados!! Para recuperá-los mande um e-mail para 'xxxx@xxx.com'. O que devo fazer?

Estou sob ataque. E agora?

- Impeça que o vírus continue se espalhando nesse computador: respire fundo e desconecte o equipamento da internet totalmente. Se possível desligue esse computador e quando religá-lo, faça-o apenas pelo modo de segurança do Windows. Veja o **tutorial**.
- Impeça que o vírus se espalhe pela rede: peça a todos que desconectem os computadores da rede e verifique cada um separadamente. Se possível desligue os computadores que não foram afetados até que eles possam passar por uma análise técnica.
- Agora que você já sabe quais computadores foram afetados, verifique opções de backup: consulte se há um backup desses arquivos e quando foi feito. Cheque ou peça para alguém checar se os arquivos do backup estão livre de vírus.
- Descubra ou peça ajuda para descobrir qual é a família do Ransomware a partir de um arquivo infectado:

Nomoreransom.org

VirusTotal.com

Id-ransomware.malwarehunterteam.com

Labs.bitdefender.com

- Pesquise ou peça ajuda para pesquisarem se existe alguma ferramenta que recupera arquivos afetados por esse Ransomware:

Nomoreransom.org Decryption Tools

Noransom.kaspersky.com

Avast.com Ransomware Decryption Tools

Emsisoft.com Ransomware Decryption Tools

McAfee.com Ransomware Decryption Tools

Quickheal.com ransomware Decrypton Tools

Trendmicro.com Ransomware Decryption Tools

- Elimine o vírus do computador antes de reverter o backup ou utilizar uma das ferramentas de decriptografia: antivírus comuns não são suficientes para parar o Ransomware e outros malware avançados sozinhos. Listamos abaixo três opções para serem consideradas:

1. Formatar e reinstalar o sistema do zero: essa é única forma de ficar 100% seguro que o vírus foi eliminado. Porém isso apaga todos os arquivos e elimina a possibilidade de fazer uma perícia forense para descobrir como o ataque foi realizado.

2. Instalar um aplicativo antimalware que tenha vacina para esse tipo de Ransomware. Normalmente são software pagos.

Malwarebuster.com

Malwarebytes.com

3. Solicitar a um profissional com experiência em detecção e mitigação de malware para verificar a máquina. Nem todo profissional de TI vai ter essa experiência. Considere contratar uma consultoria especializada em segurança da informação.

- Faça o backup dos arquivos infectados e guarde para o futuro: mesmo que hoje em dia não existam ferramentas que restaurem seus arquivos não perca as esperanças. Guarde uma cópia dos arquivos infectados em um HD externo.

Pagar ou não pagar?

"Pagar o resgate nunca é recomendado, principalmente porque não há garantia de que isso solucione o problema. Um número considerável de problemas podem surgir depois de pagar o resgate. Por exemplo, algum componente de recuperação do malware pode ter um bug que faça com que os dados cifrados fiquem irremediavelmente perdidos, mesmo com a chave de decifragem correta.

Adicionalmente, se o resgate for pago, prova aos criminosos que o Ransomware é efetivo. Como resultado, os criminosos irão continuar a desenvolver sua atividade à procura de novas formas de explorar sistemas, realizar mais infecções e arrecadar mais dinheiro."[1]

1 - https://www.nomoreransom.org/pt/ransomware-qa.html

NEGOCIANDO COM O ATACANTE

Se sua organização escolher negociar e pagar o resgate dos dados, é imperativo que você siga recomendações de segurança. Listamos os seguinte cuidados:

- Utilize uma conta anônima para se comunicar com o atacante. Recomendamos usar ferramentas de anonimato como Protonmail a partir do navegador TOR. **Veja o tutorial**.
- Nunca envie os arquivos infectados para o atacante. Isso pode ser uma estratégia para a pessoa determinar se os arquivos são valiosos e aumentar o preço do resgate. Sempre negocie a compra de uma chave que o atacante lhe enviará e nunca o contrário.
- Uma vez que está com a chave em mãos, prepare um computador para executar essa ferramenta. Esta deve ser uma máquina totalmente separada da rede e da internet e deve ter nela uma cópia de todos os arquivos infectados. Às vezes chaves compradas funcionam uma única vez, por isso é importante que todos os arquivos estejam contidos nessa mesma máquina. Depois do uso, copie os arquivos para um lugar seguro e formate o computador utilizado.
- Considere formatar as máquinas da organização e avalie a possibilidade de mudar para o Sistema Operacional Linux, pois os malwares mais populares são para Windows. Mas tome cuidado para não fazer uma mudança brusca e se arrepender depois. Recomendamos testar com algumas pessoas para avaliar se essa solução funcionaria para sua organização.

Como se prevenir?

Não há receitas prontas de como se prevenir de um ataque de Ransomware. Fortalecer a segurança digital de sua organização é um esforço transversal que envolve tanto boas práticas pessoais quanto uma infraestrutura segura e bem configurada. Nas sessões a seguir apresentaremos diversas formas de se proteger, porém alguns tópicos são prioritários na prevenção contra o Ransomware.

- Backup e política de backup;
- Configure seus servidores locais. Nunca deixe portas RDP (acesso remoto) abertas para a internet;
- Crie uma rede Wi-fi de visitantes apartada da rede de computadores da organização;
- Cuidados com e-mails;
- Antivírus atualizado em todos os computadores;
- Considere mudar o sistema operacional dos computadores para Linux;
- Explique para a equipe a importância de ter cuidado ao abrir links de e-mails e mensagens instantâneas. Se possível crie acordos para isso, pois é uma porta de entrada para ataques e a responsabilidade pela autoproteção deve ser compartilhada.

PARTE 2

SEGURANÇA ORGANIZACIONAL

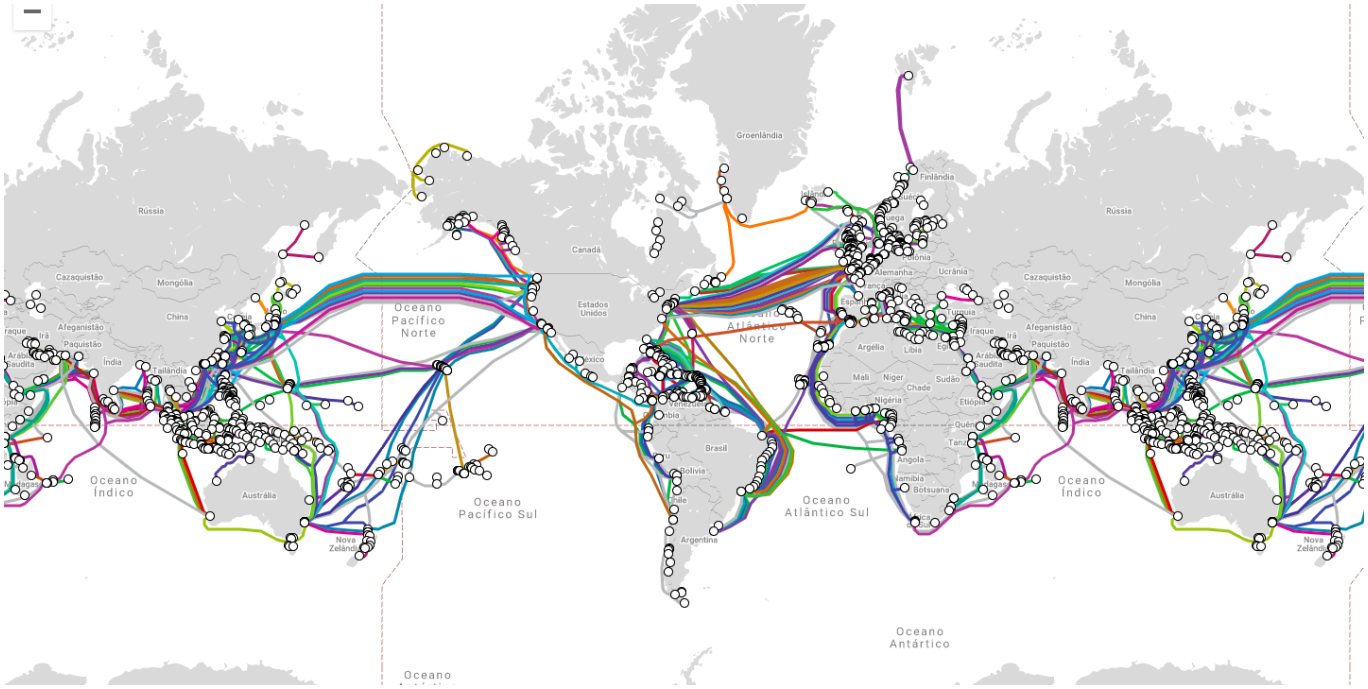
Entendemos que o debate sobre a segurança deve estar inserido na estratégia e estrutura organizativa de um grupo, e isso deve acontecer após uma análise de suas atividades, vulnerabilidades e riscos.

Não existem receitas prontas ou cartilhas de segurança que servem para todos. A segurança organizacional é feita sob medida: são acordos que consideram as formas de tomadas de decisão, o contexto político e a composição da equipe de cada grupo.

Nesse guia iremos falar sobre vários aspectos que configuram a segurança digital da uma organização e os conceitos que estão atrás de algumas das suas vulnerabilidades.

Existem perguntas muito comuns que se deve fazer em relação à segurança. Neste texto elas estão dentro de quadros em cada uma das sessões. Boa leitura.

2 - A internet e as infraestruturas digitais das organizações



Fonte: submarinecablemap.com

Imaginamos a "nuvem" e nossos arquivos digitais como coisas virtuais, não físicas, intocáveis e possivelmente distantes. Talvez também por isso consideramos que não é necessário saber o que faz esta tecnologia funcionar. É uma máquina e confiamos nela.

Na verdade a tecnologia na qual que nos apoiamos para fazer nosso trabalhos é composta de coisas físicas: chips, condutores, cabos, computadores, servidores e roteadores. Também de pessoas que traba-

lham para criá-la e mantê-la, assim como estruturas de poder que são proprietárias e reguladoras desse bem aparentemente imaterial e apolítico.

A comunicação e produção de conteúdo das organizações que lutam por direitos estão estabelecidas nessas estruturas e é necessário olhar para elas de forma crítica.

A internet e as infraestruturas que usamos para fazer nosso trabalho possuem camadas tecnopolíticas e também precisam de atenção e cuidado coletivo para funcionarem a nosso favor e para estarmos mais protegidas. É sobre tudo isso que falaremos a seguir.

3 – Servidores e nuvens

O que é um servidor?

É um computador que guarda e disponibiliza arquivos, conteúdos de um site, um serviço de e-mail, aplicativo de chat, entre outros. Qualquer computador - teoricamente - pode ser um servidor, porém para garantir que esses serviços estarão sempre funcionando é comum que esses computadores sejam bem potentes, consequentemente mais caros que computadores pessoais, e que estejam ligados 24h por dia.

3.1 - Servidores locais

Quando necessitamos compartilhar arquivos dentro de um grupo, faz sentido centralizar esses arquivos em um servidor. Esse equipamento servirá para armazenar toda informação que a equipe precisa acessar e também pode ser usado para hospedar e disponibilizar serviços.

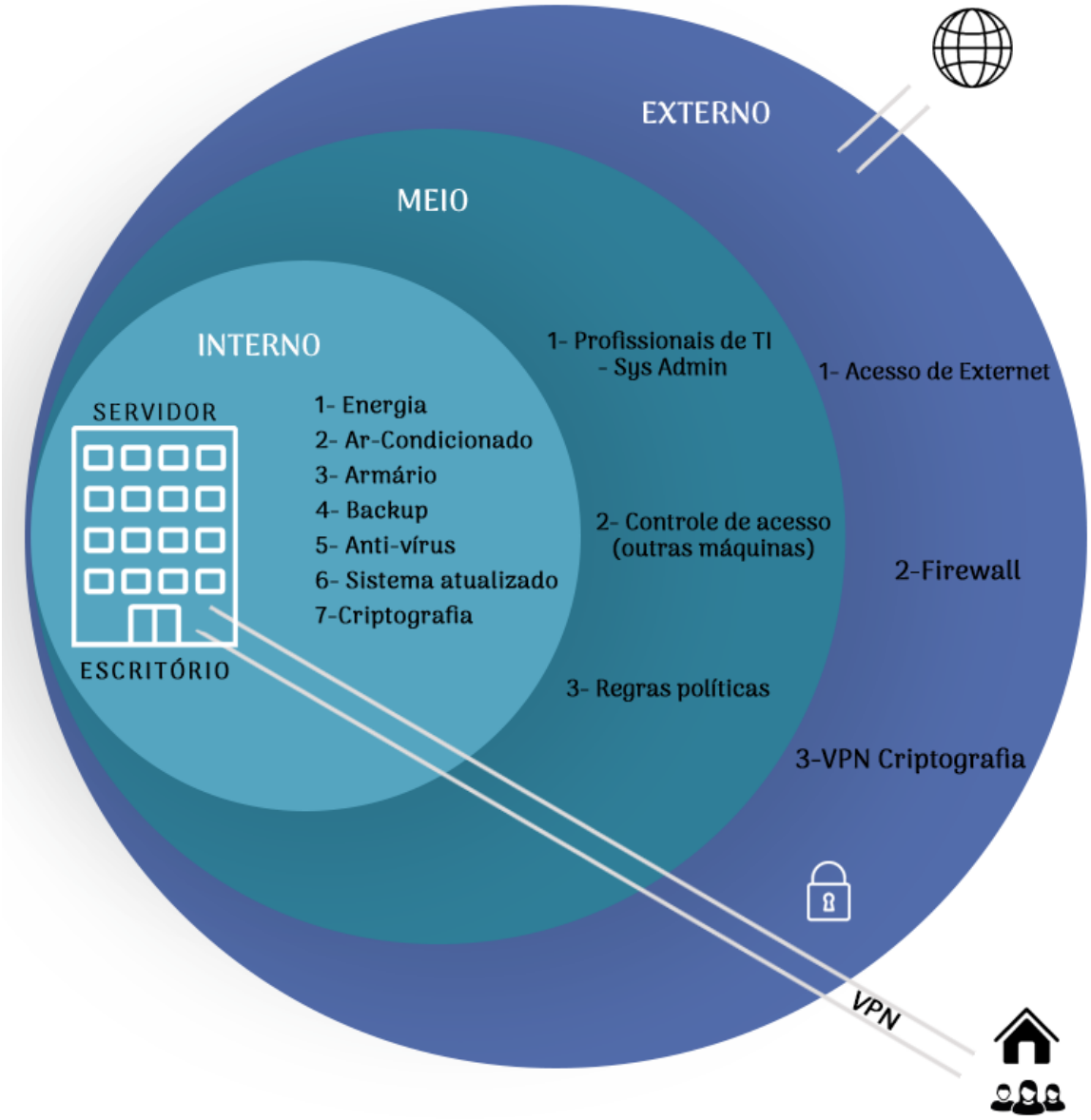
Um servidor requer muitos cuidados na segurança, pois será o grande "armário digital" da organização. Para isso não podemos pensar nele como um "computador reserva" que pode ser utilizado para funções gerais. Seu uso deverá ser exclusivo para a função que foi designado e alguns cuidados especiais devem ser tomados.

PERGUNTAS QUE DEVEM SER FEITAS:

1. Quem precisa acessar diretamente o seu servidor? Todos os computadores? A rede de visitantes? Toda a internet?
2. O que acontece se as informações do servidor forem apagadas ou perdidas? Existe uma cópia?
3. Existe antivírus? O que acontece se alguém conectado na rede baixar um arquivo infectado?
4. O servidor está em um local seguro? Ou está em um lugar que todas as pessoas acessam?
5. Quem é a pessoa que cuida do servidor? A organização tem acordos de confiança com ela?
6. O servidor é acessado a partir da internet? Por quem? O que impede outros de entrarem pela mesma porta de acesso?

Camadas de segurança de um Servidor Local:

Para facilitar a visualização da segurança de um servidor local vamos apresentá-la em camadas, desde uma visão interna, organizacional e externa.



Camada 1 - Interna

Essa é a camada relativa ao *hardware* e *software* do servidor e onde ele está fisicamente. Para proteger essa camada verifique:

Local do servidor:

O local precisa ter energia e refrigeração constante. O ideal é ter um *no-break* e um ar-condicionado exclusivo para o seu servidor. Se possível o lugar do servidor deve ser fechado com chave e o acesso deve ser somente para as pessoas autorizadas.

Sistema do servidor:

Sempre utilize a versão mais atualizada do sistema operacional, pois quando uma vulnerabilidade é descoberta as atualizações vão corrigi-la.

Se utilizar servidores Windows não esqueça do **Antivírus**.

Use uma **criptografia de disco** em seu servidor para proteger em caso de roubo.

Backup:

Cuidado com o seu **backup**; é muito importante ter cópias de segurança dos arquivos do servidor – mas é ainda mais importante que esse backup seja externo. Um HD conectado não protege a organização de ameaças como *Ransomware*, furtos ou incêndios. Considere guardar esse backup em um servidor na nuvem de sua confiança.

Camada 2 - Meio

Essa é a camada que tem a ver com o como a organizaçao cuida de seu servidor.

Profissional técnico:

É importante ter ajuda de um profissional de confiança e que tenha experiência com infraestrutura de servidores para fazer a manutenção. Cuidar de um servidor não é a mesma coisa que cuidar de um computador comum e não é toda pessoa técnica que possui esse conhecimento. Você precisará de um '**sysadmin**'; uma pessoa responsável pela configuração e manutenção dos servidores da rede. Esse profissional terá acesso a todos os arquivos dentro do servidor, então também consideramos essencial que seja estabelecido um acordo de confidencialidade.

Camada 3 - Externa

Essa e a camada mais externa, que cuidará da segurança do servidor com a internet.

Acesso via internet:

Instale um *Firewall* (muro de fogo) para limitar quais acessos devem entrar ou sair da sua rede. Recomendamos a distribuição **Pfsense**.

Acesso de manutenção:

Somente pessoas de sua confiança devem poder acessar o servidor, tanto fisicamente quanto remotamente. Cuide da segurança dos acessos via internet da rede do seu servidor.

A maneira mais recomendada de acesso remoto é através de uma VPN (Virtual Private Network).

O QUE É UMA VPN

A VPN cria um túnel criptografado entre dois computadores, ou nesse caso, entre o computador da pessoa que está remota e a organização. Dessa forma basta a pessoa "ligar" esse túnel, e será como se estivesse fisicamente dentro da sede. Saiba como configurar um servidor de VPN para sua organização **nesse link**.

Há diversos aplicativos que permitem o 'suporte remoto' como o Teamviewer ou Anydesk. Apesar da facilidade de utilizar esses aplicativos, não recomendamos essas soluções para servidores, pois além de serem softwares proprietários que podem estar coletando dados sem nosso consentimento, usar soluções de mercado abre possíveis vulnerabilidades que os *malwares* podem explorar[1].

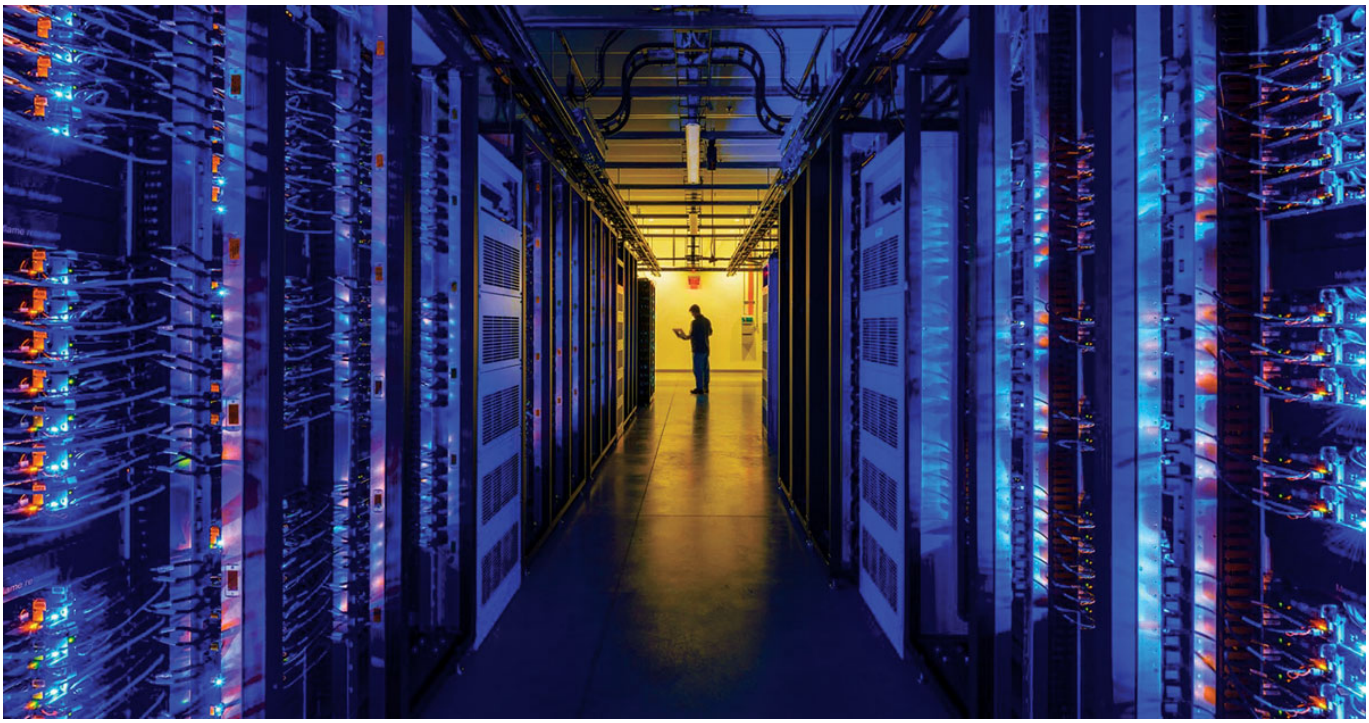
Tome atenção com **RDP**, é uma ferramenta muito usada por ser nativa do sistema Windows, mas ela abre muita brechas de segurança. Só use o RDP através de uma VPN.

1 - https://www.securityweek.com/backdoor-abuses-teamviewer-spy-victims
https://blog.avast.com/ransomware-attacks-via-rdp

3.2 - Servidores na nuvem

O que é uma nuvem?

Uma nuvem é um servidor que está localizado em um **datacenter** em algum lugar no mundo. Esse servidor é "alugado" para que outras organizações possam instalar seus próprios serviços, como websites, sistemas financeiros ou armazenar arquivos.



Fonte da imagem: 123rf.com

Como usar uma nuvem segura?

Um servidor na nuvem é um servidor de outra pessoa ou empresa. Para ter segurança e privacidade, é necessário usar serviços de confiança, com políticas de privacidade coerentes e com criptografia.

A criptografia é uma tecnologia que usa algoritmos e cálculos para embaralhar as informações, ou seja, para deixar as informações ilegíveis para quem não tem o acesso correto. Há vários tipos de criptografia: de arquivos, de e-mail, de transporte, de dispositivo, etc. As aplicações são diversas, mas quando bem implementadas o resultado é a privacidade das nossas informações.

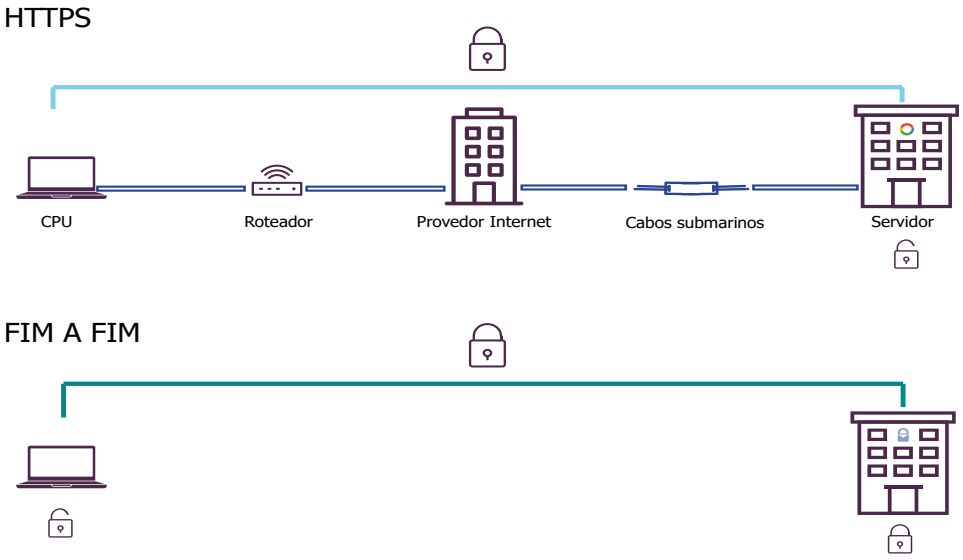
Criptografia fim-a-fim: como se comunicar seguramente na nuvem

Felizmente, desde 2014, a maioria dos serviços de comunicação já usam uma camada de criptografia de trânsito, ou HTTPS. Essa camada de criptografia garante que as informações fiquem protegidas durante seu percurso, não podendo ter seu conteúdo interceptado no meio do caminho por curiosos.

No entanto é importante lembrar que a criptografia de trânsito não protege nossas mensagens dentro do servidor de e-mail ou de chat onde estão armazenadas.

Quando enviamos um e-mail usando o Gmail, uma cópia de nossas mensagens fica legível no servidor e podem ser acessadas pela Google para vender serviços, e também através de **pedidos judiciais**.

Uma forma de garantir que as informações fiquem seguras, mesmo dentro de servidores de empresas, é usando programas que utilizem criptografia fim-a-fim. Esse tipo de criptografia garante que apenas as pontas – ou seja, destinatário e remetentes, tenham acesso ao conteúdo da mensagem.



4 – Ferramentas de comunicação segura

4.1 - E-mail

Os e-mails são ferramentas muito importantes para organizações e são, na maior parte das vezes, o principal canal de comunicação. Muitas organizações se apoiam em serviços de e-mail oferecidos pelas hospedagens de *sites* como Locaweb e Hostgator, ou por serviços "gratuitos" do Google. É necessário olhar para esses serviços e suas políticas de privacidade com cautela.

PERGUNTAS QUE DEVEM SER FEITAS:

1. Onde fica hospedado nosso servidor de e-mail?
2. Quem tem acesso a nossos e-mails?
3. Qual o papel dos mensageiros instantâneos em nosso organização?
4. Que tipo de informação pode circular por aplicativos de celular?
5. Quais aplicativos são institucionais e quais não são?

Protonmail e Tutanota

Poucas organizações terão infraestrutura para manter um servidor de e-mail próprio com segurança e confiança. Tendo isso em mente, recomendamos dois serviços de e-mail com criptografia que são muito fáceis de usar. Esses serviços fornecem acesso via *web* ou *smartphone*, e se você enviar uma mensagem para outro usuário que utiliza o mesmo provedor, ele aplica automaticamente a **criptografia fim-a-fim**. São serviços que podem ser contratados e usados com o domínio da sua organização (@organização.com) e apesar desse recurso ser pago, ambos os projetos oferecem descontos para ONGs.

Protonmail.com **Tutanota.com**

Contas de email + GPG

Existem outras formas de fazer a criptografia fim-a-fim usando qualquer provedor de e-mail; seja ele comercial como Gmail e Hotmail ou ativista como as seguintes.

Riseup.net **Mayfirst.coop**

Autistici.org

Isso é feito através do uso de um cliente de e-mail chamado Thunderbird e *plugins* de criptografia como Enigmail. Não há custo para utilizar esse recurso, porém toda a sua equipe deve ser treinada no uso desses aplicativos. O passo a passo para isso pode ser encontrado em **Emailselfdefense.fsf.org.**

CUIDADOS COM E-MAIL: PHISHING

O phishing é um tipo de fraude que ocorre por meio de mensagens que tentam convencer o usuário a baixar um arquivo malicioso ou fornecer informações pessoais. Essas mensagens simulam a comunicação oficial de uma instituição pública, como um banco, uma empresa ou um site popular.

Apesar de ser uma ameaça muito conhecida, essa é uma das principais formas que malwares avançados como Ransomware e programas espiões entram dentro das organizações.

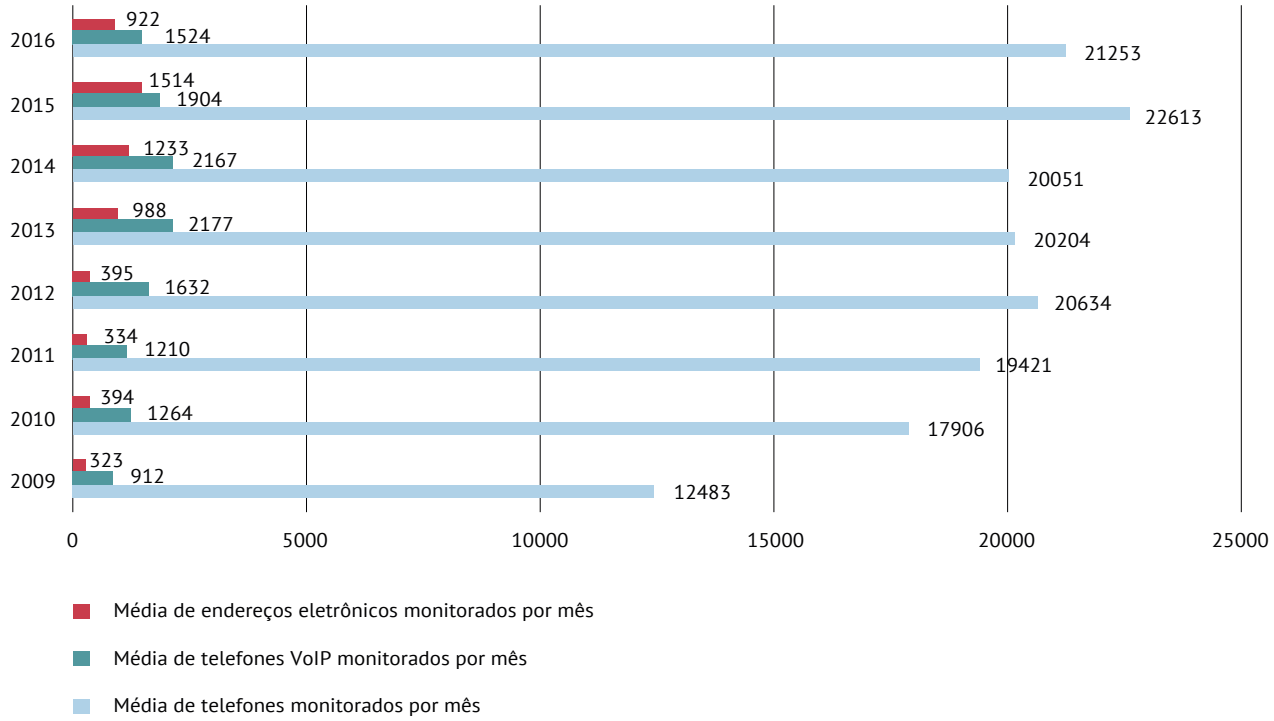
A principal prevenção é informar e treinar os usuários nos cuidados com os e-mails. Leia mais nessa cartilha: **Cartilha.cert.br/golpes**

4.2 - Mensageiros instantâneos e videoconferências

Whatsapp e Skype

Além de e-mails, os chats e vídeoconferências como *Whatsapp* e *Skype* (VoiP) se tornaram ferramentas de comunicação para um grande número de organizações. Apesar de muito populares, esses programas deixam a desejar em privacidade. São programas que pertencem a empresas e que já apresentaram casos de grampos, espionagem em massa e revelação de informações.

MÉDIA MENSAL DE ALVOS MONITORADOS POR ANO



Fonte: Vigilância sobre as comunicações no Brasil

Além disso, por serem programas muito populares, são alvos de ataques de *Malwares* e tentativas de golpe. Veja essas matérias sobre o Skype[1] e sobre o Whastapp[2].

Até mesmo a criptografia fim-a-fim implementada pelo Whatsapp não pode ser considerada uma forma efetiva de segurança, porque se trata de um programa de código fechado. Não há como a sociedade civil auditá-lo, ou seja, não há como garantir que a criptografia foi bem implementada nem descobrir quais dados estão sendo coletados de nossos celulares e computadores.

Apesar dos problemas apontados, são programas muito populares e por isso é também necessário cuidar de sua segurança. Verifique as recomendações de boas práticas para senhas e cuide das configurações de privacidade dos aplicativos.

1 - http://techrights.org/wiki/index.php/Skype_is_Spy_Campaign;
https://www.cbsnews.com/news/trojan-opened-door-to-skype-spying/
https://www.zdnet.com/article/syria-pushing-malware-via-skype-to-spy-on-activists/

2 - https://olhardigital.com.br/noticia/sergio-moro-se-reune-com-executiva-do-whatsapp/83091
https://www1.folha.uol.com.br/poder/2019/02/bolsonaro-fala-com-equipe-pelo-whatsapp-mesmo-com-telefone-criptografado.shtml

Quadro comparativo de aplicativos de mensagem

Fonte: https://marialab.org

Signal

O Signal é um aplicativo para Android, iOS, e Desktop que faz uso de criptografia de ponta a ponta, permitindo que os usuários enviem mensagens de grupo, texto, imagens, áudio, vídeo e chamadas telefônicas encriptadas entre usuários do Signal.

Conheça o projeto: **Signal.org**

Instale o Signal para **Windows, Linux, Mac, Android** ou **Iphone**.

Wire

O Wire oferece chamadas de voz criptografadas, chamadas de vídeo e mensagens com criptografia de ponta a ponta. Outros aplicativos como Signal e WhatsApp exigem que os usuários se registrem no serviço com um número de telefone. Esse movimento tem sérias implicações de privacidade para aqueles que preferem não dar um número pessoal antes de iniciar uma conversa. Usando Wire, você pode simplesmente se registrar com um e-mail e buscar as pessoas no aplicativo por apelidos como @grinch37. Esse aplicativo também possui contas pagas, com recursos adicionais, para organizações.

Conheça o projeto: **Wire.com**

Para usar no seu **navegador**

Instale a versão para **Android**

Instale a versão para **Iphone**

Jitsi

O Jitsi não utiliza criptografia fim-a-fim, porém é um projeto ativista e que permite autonomia. Sua própria organização pode ter um servidor de Jitsi para total independência em suas reuniões online ou utilizar servidores de grupos ativistas que se comprometem a não coletar informações sobre as videochamadas. Pode ser utilizado online direto no navegador, nos computadores desktop, ou em celulares, com um aplicativo disponível para Android e Iphone.

Para usar no seu **navegador**

Instale a versão para **Android**

Instale a versão para **Iphone**

4.3- Arquivos na nuvem

Sua própria nuvem:

Em vez de usar um serviço de hospedagem de arquivos que pertence a uma empresa, sua organização pode ter sua própria nuvem. **Nextcloud** é uma alternativa ao Google Drive, Docs e Calendar, oferecendo recursos compartilhados de arquivos, calendários, tarefas e criação de pastas públicas.

A principal diferença é que o Nextcloud precisa ser instalado em um servidor, o que nos dá muito mais autonomia em termos de espaço e controle de acesso. Caso sua organização não tenha recurso para equipamentos e pessoas especializadas, há alguns grupos parceiros que oferecem o serviço já pronto e com manutenção incluída em um pagamento mensal.

Maadix.net (espanhol)

Greenhost.net (inglês)

Rios.org.br (português)

Primeiros passos

Caso busque algo mais simples, é possível utilizar o **Mega.nz**. Mega é um sistema de hospedagem de arquivos, mas que diferente do Google Drive possui criptografia fim-a-fim. Dessa forma, os arquivos armazenados não são acessíveis nem mesmo pelos proprietários do sistema.

Para usar no seu **navegador**.

Transferência temporária de arquivos

Muitas vezes precisamos enviar arquivos grandes para a internet sem o objetivo de guardá-los, apenas para que outra pessoa tenha acesso a eles. Sites como Dropbox, Wetransfer e outros ajudam nessa tarefa, mas são proprietários e seus termos de serviço não protegem a privacidade dos usuários.

Algumas alternativas seguras:

https://send.firefox.com : até 2.5Gb, permite definir um tempo de expiração.

https://share.riseup.net : Até 50MB, expira automaticamente depois de 7 dias.

5 – Segurança dos equipamentos

PERGUNTAS QUE DEVEM SER FEITAS:

1. Existe uma cópia de segurança (backup) das informações? Onde ela está? Quem é responsável por ela? Com que frequência a cópia é feita? Existe algum 'Plano B' caso esse armazenamento falhe?
2. Quem tem acesso ao backup? Ele está criptografado?
3. Qual o papel dos mensageiros instantâneos em nossa organização? Quem tem acesso ao backup? Ele está criptografado?
4. Os computadores com Windows têm antivírus?

5.1- Backup

O que é?

O backup nada mais é que uma cópia de segurança. Há vários locais onde podemos salvar os backups: "offline", como HD externo, pen drive e o servidor interno da organização; ou "online" em um servidor contratado por nossa organização na nuvem.

Backup online	Backup offline
Servidor pertence a uma empresa	Servidor pertence a sua organização
Segue as leis dos países onde estão localizados, o que pode dificultar na apreensão física de equipamentos	Sujeito às leis brasileiras e pode ser apreendido pela Polícia Federal
Se o backup não tiver criptografia, as empresas donas dos servidores terão acesso aos arquivos	Além de criptografar você pode controlar quem tem acesso físico a ele
Não permite criptografar o HD totalmente	Pode criptografar o HD completamente
Não há custo de aquisição ou instalação de servidor	Custo inicial alto
Sua organização não precisa se preocupar com danos físicos ao equipamento	Equipamentos estragam com o tempo, necessitam de energia e ar-condicionado
Tem custo mensal	Não é um serviço, portanto não tem um custo mensal de uso

Independente do tipo escolhido como principal, o importante é ter um backup atualizado e preferencialmente mais de um, online e offline.

Com que frequência devo fazer backup?

Quanto tempo de informação seria aceitável perder? Se todos os arquivos que você criou ou modificou na última semana desaparecerem, isso teria um impacto significativo? E no último mês? No último ano? Há pessoas que não podem ficar um único dia sem as alterações realizadas em arquivos. Outras podem ser mais flexíveis.

Como posso criptografar os arquivos de backup?

Recomendamos a ferramenta **Veracrypt.fr** Com ela você pode criptografar seus HD externos e pen drives ou criar pastas criptografadas com senhas fortes antes de enviá-los para a "nuvem".

5.2 - Criptografia de equipamentos

O que é a criptografia de disco?

Usar aplicativos com criptografia fim-a-fim é uma excelente medida para proteger as comunicações entre duas pessoas, mas como proteger os arquivos em nossos computadores e servidores?

Uma senha forte para entrar no sistema operacional é uma boa prática contra curiosos, mas a única forma de proteger nossos arquivos no caso de furto ou apreensão de equipamentos é habilitando a criptografia de disco. Dessa forma, todo o computador ficará criptografado e o sistema operacional apenas irá iniciar depois que você digitar uma senha.

Linux e MAC:

Ambos possuem criptografia de disco nativa. Basta configurá-la corretamente.

Para configurar no **Linux**. Para configurar no **Mac**.

Windows:

O Windows tem uma criptografia de disco chamada Bitlocker. Esse recurso opcional está disponível para servidores em todas as versões à partir do Windows Server 2008 e para computadores com Windows 7, 8 ou 10, apenas nas versões Enterprise, Pro e Ultimate. Para aprender a configurar acesse **esse link**.

5.3 - Antivírus

Todo computador com Windows na organização deve ter um antivírus atualizado. Isso é muito importante, pois mais de 80% dos vírus existentes são para Windows. No caso de Ransomware, esse número cresce para mais de 90% dos casos.

Entretanto, além de antivírus é necessário que usuários com Windows realizem constantemente atualizações de sistema. Utilizar softwares piratas que impeçam a atualização de segurança é um grande risco para todos. Considere fazer o cadastro no **Techsoup**, um programa que vende software com desconto de até 90% para organizações sem fins lucrativos.

Mac, Android e Linux precisam de antivírus?

Apesar de existir antivírus para Mac, Linux e celulares, não há o mesmo risco desses sistemas se-

rem infectados utilizando as técnicas automáticas dos vírus para Windows. Os programas maliciosos que existem para esses sistemas normalmente se passam por aplicativos legítimos em lojas de apps ou mensagens falsas enviadas por Whatsapp, e-mail e similares - os famosos **phishing**. Ou seja, utilizam técnicas de persuasão para convencer os usuários a clicar e instalar os programas. Antivírus comerciais não são efetivos contra esse tipo de ameaça e apenas a conscientização de usuários pode evitar essas infecções.

Recomendações para antivírus

Lembre-se: independente do fabricante, o mais importante é ter um antivírus atualizado em todas as máquinas com Windows.

Caso a organização opte por utilizar um serviço sem custo, recomendamos o antivírus **Microsoft Windows Defender.**

No caso de servidores ou computadores Windows que a organização considera de alto risco, reiteramos a importância de usar um antivírus pago. No programa Techsoup, há dois modelos de antivírus disponíveis:

Symantec Endpoint Small Bussiness

Bitdefender Internet Security

Uma organização com muitas máquinas pode utilizar um servidor para centralizar o gerenciamento de todas as instalações de antivírus. No projeto techsoup está disponível a versão gerenciável do antivírus Symantec, porém há outras empresas que oferecem soluções parecidas.

Symantec Endpoint Protection

6 – Celulares

PERGUNTAS QUE DEVEM SER FEITAS:

1. As informações da organização também estão nos celulares pessoais?
2. O que acontece com minhas informações se roubarem o meu celular?
3. A organização oferece um celular de trabalho?

6.1 – Cuidados no uso do celular

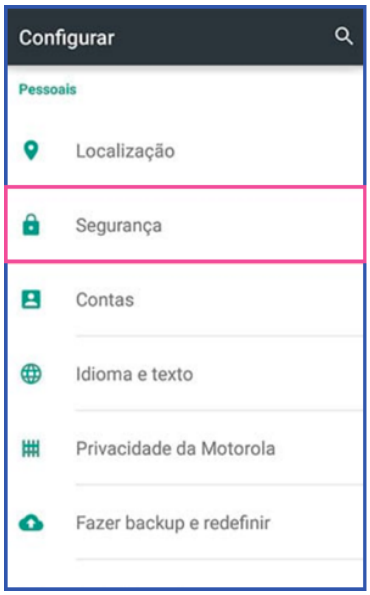
O fato de concentrarmos uma quantidade tão grande de informações em um aparelho que cabe em nosso bolso gera diversas fragilidades em nossa segurança digital. Por um lado, há uma probabilidade maior de termos esse equipamento furtado, apreendido ou danificado; por outro, carregamos conosco um "pequeno espião", que tem uma câmera, um microfone, um GPS e um sistema de antenas que está sempre triangulando nossa localização, necessário para o funcionamento básico da telefonia móvel.

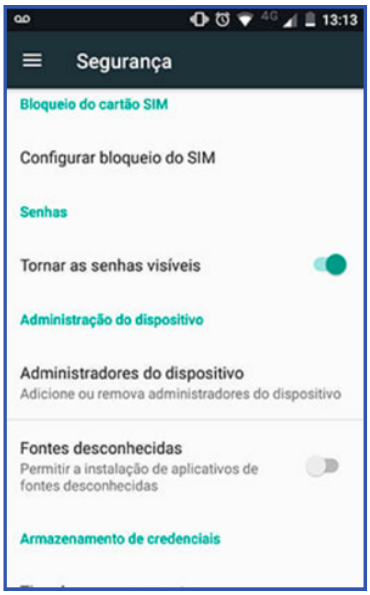
Dentro dos acordos das organizações os celulares compõem uma "área cinza", pois na maioria das vezes são dispositivos pessoais que armazenam dados da organização como arquivos, redes de contatos e grupos de conversas.

6.2 – Boas práticas

Selecionamos algumas boas práticas que podem ser inseridas nos protocolos de segurança das organizações:

1. Talvez seja óbvio, mas usar aplicativos seguros como SIGNAL e WIRE não ajuda caso alguém consiga acesso físico ao seu dispositivo desbloqueado. É muito importante proteger seu dispositivo com senha, pois as opções de arrastar e padrão não são tão seguras.





2. Evite armazenar informações confidenciais ou sensíveis no aparelho. Faça regularmente cópias de segurança (backup) das informações para um computador e use funções de autodestruição de mensagens em aplicativos quando disponíveis.

3. Apague regularmente o histórico de chamadas, mensagens, fotos, informações relacionadas a contatos, etc. Tenha certeza que você sabe o que está armazenado no seu cartão SIM, nos cartões extras de memória e na memória do aparelho.

4. Garanta que os canais de comunicação como Bluetooth e rede sem fio (WiFi) de seu telefone estejam desligados e desabilitados caso não os esteja usando.

5. Criptografe seu celular: Se o seu telefone não estiver configurado com criptografia de disco, mesmo com senha é possível que um atacante leia e copie dados do seu dispositivo no caso de perda ou furto.

Android

A maioria dos Androids modernos já vem com criptografia, veja como realizar o procedimento para celulares android anterior ao 8.0.0 **nesse link**:

Iphone

A maioria dos dispositivos modernos da Apple já encripta conteúdos como configuração padrão, com vários níveis de proteção. Mas, para se proteger de alguém que rouba fisicamente o seu dispositivo, é necessário criar uma senha. Veja mais informações **nesse link**.

Windows Phone

O Windows Phone permite a criptografia na versão 10 do sistema operacional. Veja mais informações **nesse link**.

7 - Protegendo contas e serviços

PERGUNTAS QUE DEVEM SER FEITAS:

1. Quantas contas digitais você tem? Como conseguem te achar?
2. Há alguma política de senhas seguras em sua organização?
3. A autenticação em dois fatores está habilitada nas contas mais importantes?
4. Como compartilhar senhas de forma segura entre pessoas de um mesmo departamento ou função?
5. Sua conta de rede social está bem configurada?

7.1 – Senhas

Senhas são uma parte muito importante de nossa segurança digital. Da mesma forma que boas trancas e fechaduras são as principais ferramentas de segurança patrimonial, as senhas são a principal forma de assegurarmos nossas contas e acessos.

Como fazer boas senhas?

Por muito tempo se pensou em senhas como uma única palavra. Uma senha forte, nesse caso, seria uma palavra bem complicada com caracteres especiais, letras maiúsculas e minúsculas, números e substituições. Algo como **$%P@l4vr4M&gic4_2001**.

Senhas assim podem ser complicadas para um invasor quebrar, mas também são muito difíceis de guardar. Recomendamos que você passe a ver as senhas não como uma palavra, mas como uma frase.

cadeira abacate advogado amarelo

Essa senha (com espaços!) é ainda mais segura que o palavrão anterior. Por se tratar de uma frase longa e bastante aleatória, mesmo que atacantes saibam que você se comunica em português, matematicamente será muito difícil quebrarem essa senha.

Dicas adicionais sobre senhas seguras:

- A sua senha é sua. Não conte pra ninguém, nem mesmo para profissionais de TI.
- Não use a mesma senha para tudo! Cadastramos nossas senhas em algum site e é sempre possível que esses serviços sejam hackeados. Parece improvável, mas todo ano milhares de senhas vazam na internet. Você pode verificar se teve alguma conta vazada aqui: **Monitor.firefox.com**.
- Troque suas senhas regularmente
- Não salve senhas em navegadores nem habilite o login automático. Sair ou fazer 'logoff' após usar alguma conta é tão importante quanto fechar a porta atrás de nós ao sairmos de casa.
- Não há memória que dê conta de tantas senhas seguras. Recomendamos o uso do KeepassXC para gerenciar as suas. Esse programa cria um banco de dados criptografado de senhas e pode ser compartilhado entre pessoas que precisam dividir acessos. Veja como funciona **nesse link**.

Autenticação em dois fatores (2 factor autentication)

A autenticação de dois fatores é um recurso oferecido por vários serviços online que acrescentam uma nova camada de segurança na hora do login. A ideia é que o usuário tenha uma forma adicional de autenticação caso a primeira seja comprometida. Geralmente é solicitado um código após a verificação da senha, esse código é enviado por SMS, e-mail ou aplicativo de celular.

Recomendamos habilitar o duplo fator em todas as suas contas mais importantes. **Esse site** possui links de configuração e tutoriais para você seguir.

DUPLO FATOR DE AUTENTICAÇÃO NO WHATSAPP

A configuração do duplo fator de autenticação no Whatsapp e outros mensageiros é a melhor forma de se proteger de um golpe bastante popular conhecido como 'clonagem de Whatsapp'.

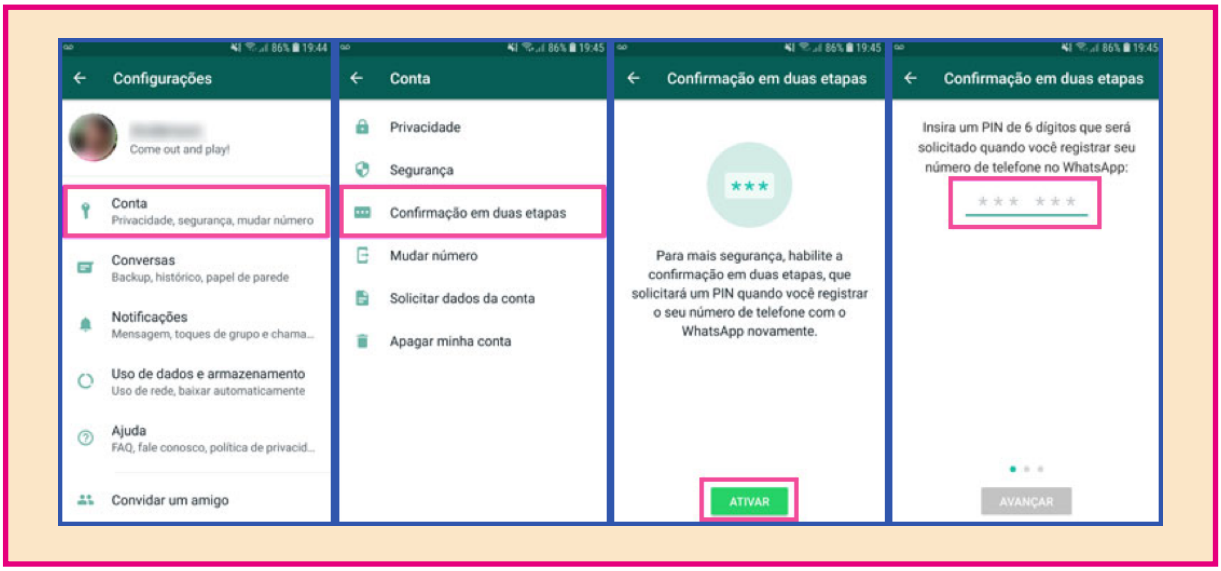
Nesse golpe, o atacante consegue acesso a sua conta através do Whatsapp web ou transferindo o número telefônico da vítima para um outro chip. Por padrão, o Whatsapp carregará automaticamente o seu perfil e contatos para um novo aparelho, porém se configurarmos o segundo fator de autenticação esse procedimento passará a solicitar uma senha.

Para ativar a confirmação em duas etapas no WhatsApp abra: ***Configurações (Android) / Ajustes (iOS) > Conta > Confirmação em duas etapas > ATIVAR.***

Ao ativar esse recurso, recomendamos inserir seu endereço de e-mail. Caso você esqueça seu PIN de seis dígitos, o Whatsapp enviará um link a esse e-mail para desativar a confirmação em duas etapas. Faça o mesmo no Telegram seguindo **essas instruções**.

7.2 - Segurança nas Redes Sociais

Quase todas as pessoas possuem perfis nas redes sociais como Facebook, Twitter e Instagram.



Alguns as usam apenas para lazer, outros manifestam opiniões políticas e trabalham para fortalecer a comunicação de sua organização. Independente de nosso uso, somos todos reféns dos "padrões da comunidade" quer concordemos com eles ou não.

As responsáveis pela comunicação de uma organização devem tomar medidas especiais para proteger suas contas, mas não apenas elas. As redes sociais tornaram-se importantes ferramentas de engenharia social, há muitos casos de violência online devido a posição política ou atuação em organizações que lutam pelos direitos humanos.

Recomendamos a leitura do texto **nesse link** para promover a reflexão de como a proteção de nossas redes sociais devo integrar os protocolos organizacionais:

Dicas de segurança para Redes sociais

1. Escolha senhas fortes e habilite a autenticação de 2 fatores. Isso vai dificultar que atacantes ganhem acesso indevido ao seu perfil e derrubem sua conta.
2. Verifique todos os dispositivos conectados. Desconecte qualquer equipamento desconhecido.
3. Configure corretamente quem pode ver as suas publicações.
4. Muy amigos, pero no mucho. O Facebook não é uma mesa de bar. Seja cauteloso com as pessoas que adiciona como amigos.
5. Proteja e disfarce informações. A maioria dos sites permite o cadastro com um 'nome social', o que dificulta que pessoas mal intencionadas consigam obter dados formais como número de documentos e telefones. Não divulgue seu endereço, sua rede de amigos, membros da sua família, etc.
6. Crie acordos de Privacidade e Confidencialidade. Eles deixam explícito o que pode ser publicada e por quem. É importante fortalecer a comunicação sem enfraquecer a segurança digital da equipe.

Instruções de segurança em cada rede social

Nesses links você acessa instruções de segurança específicas para essas redes sociais.

Facebook **Twitter**

Instagram **Linkedin**

8 - Conclusão

Quando olhamos para nossas vulnerabilidades e riscos é normal sentirmos uma sensação de ansiedade e até mesmo de paranoia. No entanto é apenas olhando para essas ameaças que conseguimos perceber as coisas que devemos cuidar para termos maior segurança.

Nesta cartilha, focamos as dicas e estratégias no aspecto digital da nossa segurança, mas para nos protegermos nas organizações é necessário considerar as dimensões integrais da segurança, como a segurança patrimonial e psicossocial.

Por exemplo, em alguns casos o trabalho nas organizações inclui viagens e participação em eventos, e esses acontecimentos podem envolver riscos e ameaças. Para que a equipe fique mais segura nesses trajetos é importante que se estabeleça acordos e protocolos com pessoas da organização para que estas possam monitorar a sua segurança.

Imprevistos podem acontecer e nesses casos de crise é extremamente importante ter respostas rápidas, como contatos de emergência e informações de logística, e até mesmo informações relativas à situação de saúde da pessoa da equipe.

Sair da nossa zona de conforto é necessário para levantar nossas defesas, mas sem nos prejudicar caindo em situações paralisantes.

Por isso consideramos que a segurança organizacional é um conjunto de ações de proteção planificadas numa linha do tempo e que devem ser feitas através de acordos e cuidados coletivos.

É importante que existam pessoas dentro da organização para acompanhar a aplicação de protocolos e acordos e que essa atividade esteja alinhada com as estratégias da organização.

Cuidar da segurança não é uma tarefa que pode ser realizada por uma única pessoa ou departamento. É uma responsabilidade de todes.

GLOSSÁRIO

- **Malware**: malware é um tipo de programa que realiza ações não autorizadas no seu computador, é o popular "vírus".
- **Bitcoins**: é uma criptomoeda descentralizada ou um dinheiro eletrônico para transações ponto a ponto.
- **Metadados**: são dados sobre outros dados. Um item de um metadado pode dizer do que se trata aquele dado, geralmente uma informação inteligível por um computador.
- **No-Break**: é um sistema de alimentação secundário de energia elétrica que entra em ação, alimentando os dispositivos a ele ligados, quando há interrupção no fornecimento de energia primária.
- **Sysadmin**: em português significa Administrador de sistemas, é uma pessoa encarregada por manter e operar computadores e/ou a sua rede.
- **RDP**: Remote Desktop Protocol (ou somente RDP) é um protocolo multicanal que permite que um usuário se conecte a um computador rodando o Microsoft Terminal Services (antigo Terminal Service).
- **Datacenter**: é um local onde estão concentrados os sistemas computacionais de uma empresa ou organização.
- **VoIP**: (Voice Over Internet Protocol) é fazer ligações de voz usando a Internet.

Realização

Texto e pesquisa: Fer Shira e Carla Jancz

Diagramação: Thais Jussim

Revisão: Patricia Cornils

Infográficos: Tatiane da Costa Carvalho

Recursos gráficos

Freepik.com

The Noun Project

Agradecimentos

Agradecemos a todas as organizações e pessoas entrevistadas por seu tempo e confiança.

Camila Veiga e Fatima Nascimento por todo o apoio durante as oficinas.

Demais manas da Marialab, principalmente Lai nossa querida designer.