WWW.INCENTEA.COM | 2020

15 Abril 2020

PESSOAS COM SOLUÇÕES

inCentea TECNOLOGIA DE GESTÃO 30 ANOS

Bruno Braz
Lúcio Crespo
Susana Marrazes

Temas “quentes”

Cada organização está a adaptar-se a esta realidade e anos cabe-nos a tarefa de ajudar e orientar não apenas no que são as melhores práticas mas também de alertar dos perigos e da execução de processo não planeados

Temos as soluções para que as empresas não sejam afetadas por causas externas, onde os colaboradores necessitam de trabalhar remotamente.

Teletrabalho

Têm que ser definidos os serviços a serem disponibilizados remotamente

Têm que ser configuradas ligações remotas no datacenter .

É necessário rever licenciamentos de software

Tem que se assegurar que os servidores suportam maior quantidade de utilizadores remotos

Segurança

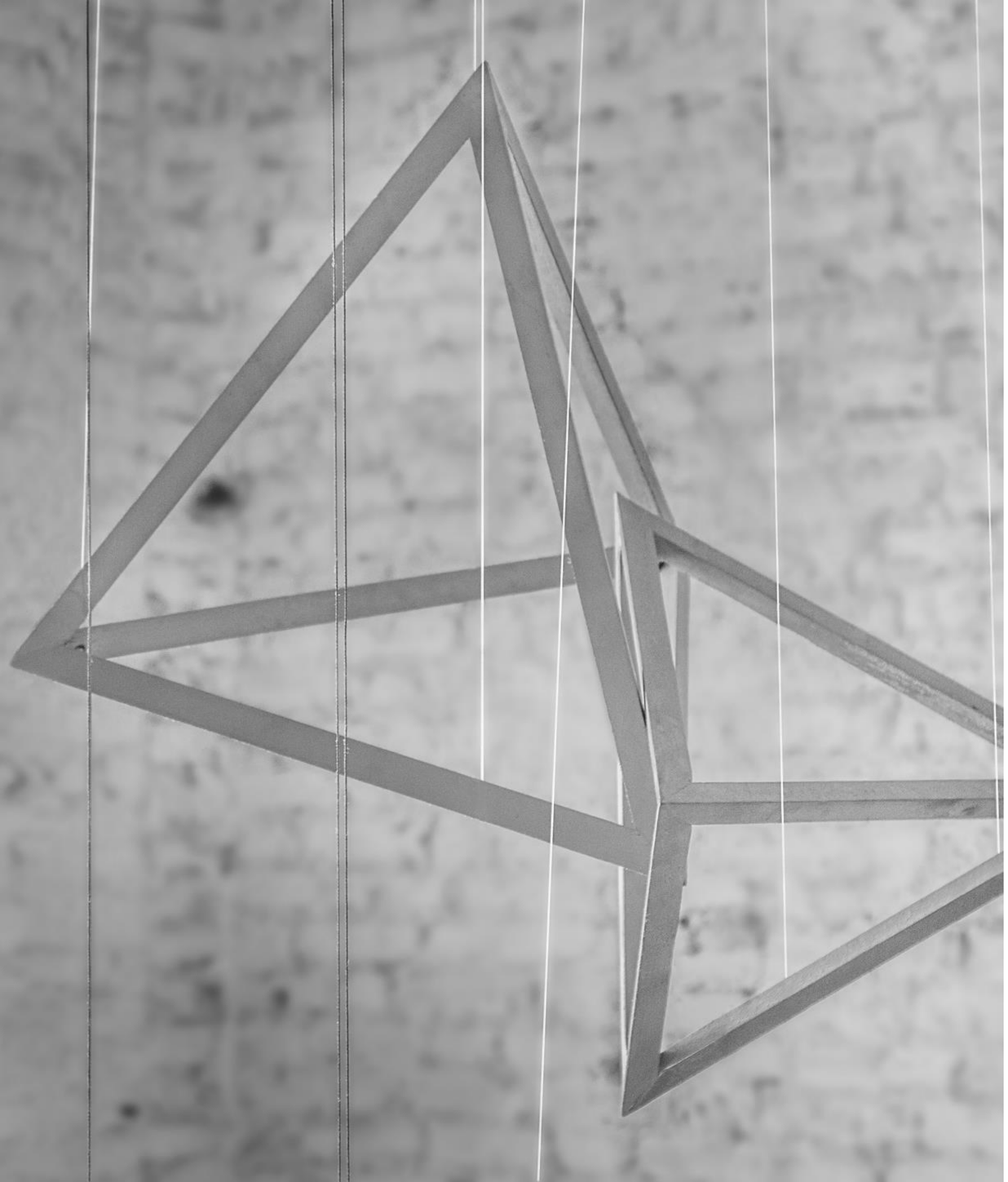
As proteções de perímetro não chegam agora que cada colaborador é um novo perímetro.

As empresas podem não ter ninguém mas os equipamentos continuam a funcionar e não pode haver quebra de serviço

As politicas de segurança tem que ser revistas porque os cenários das empresas mudaram.

Conetividade

Tem que se garantir a conetividade à internet assim como largura de banda para suportar muitas mais ligações remotas



Questões dos clientes:

- O meu servidor está preparado para Teletrabalho?
- As minhas comunicações são seguras?
- A Pirataria em tempos de Covid19
- A produção ou a empresa fechou. E o meus dados?
- Como configuram hardware novo sem intervenção física?
- Porque agora mais que nunca é preciso software contra ameaças desconhecidas. InterceptX e TDR nos postos de trabalho
- As aplicações na cloud não precisam de manutenção? E são 100% seguras?

Conceitos

Informação

É um **Ativo** “Qualquer coisa que tenha valor para a organização” importante ao negócio de qualquer organização e portanto tem de ser devidamente protegido.

Segurança e proteção de rede

As preocupações com a segurança devem ser mantidas e minimizar os riscos de perca de Informação

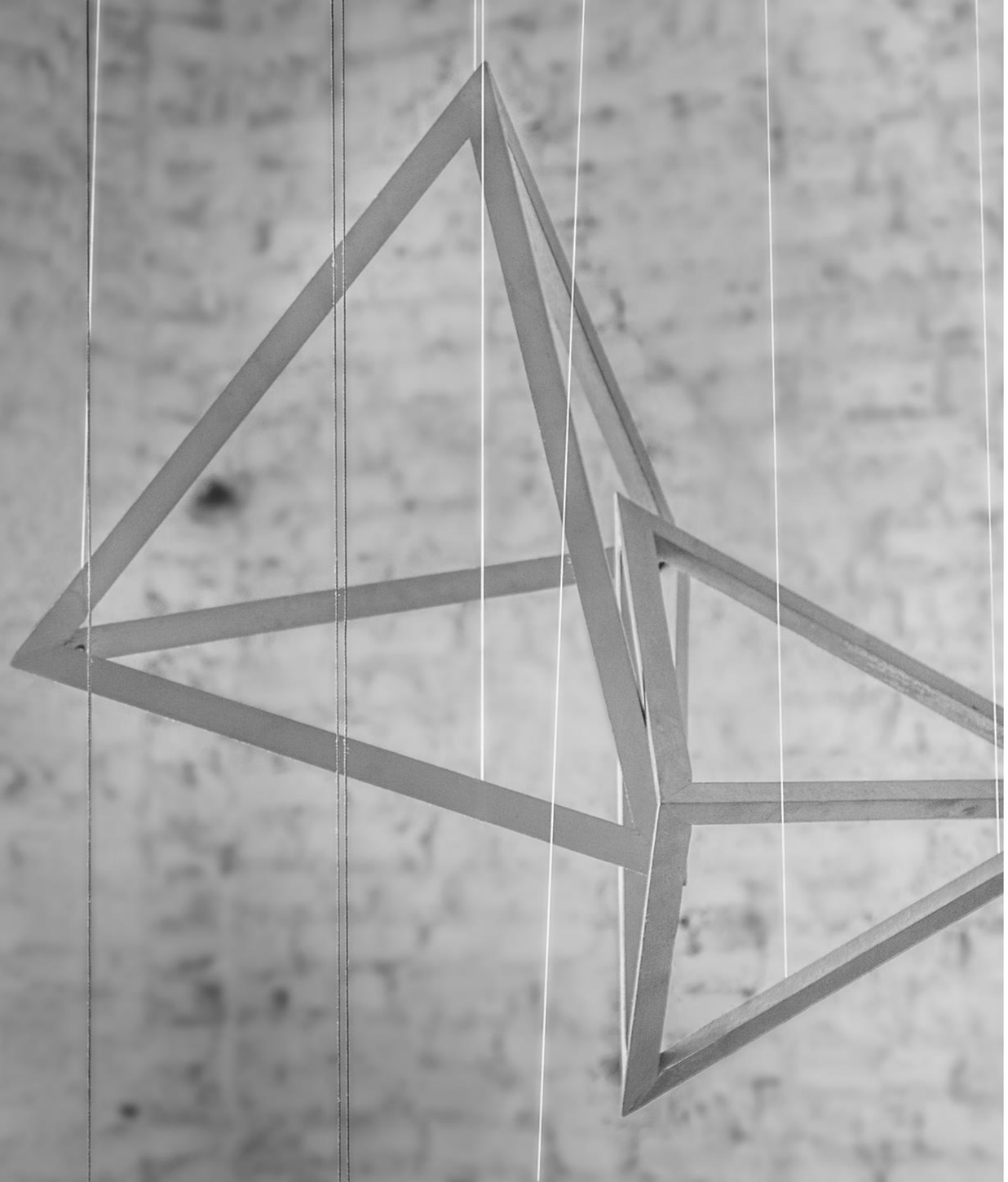
O teletrabalho apresenta novos desafios

Infraestrutura

Origem: Latim.

Infraestrutura é o alicerce interno de uma empresa.
Existe para disponibilizar serviços e recursos que permitam solucionar os problemas dos clientes.

CASO 1
Disponibilizar aplicações aos colaboradores remotos



Identificar as aplicações

Quais os serviços a disponibilizar e onde está a sua instalação?

A aplicação é WebBased? ou ClientServer?

Desempenho

O acesso a aplicações e serviços não pode afetado por problemas de velocidade ou estabilidade nas comunicações.

Gestão centralizada

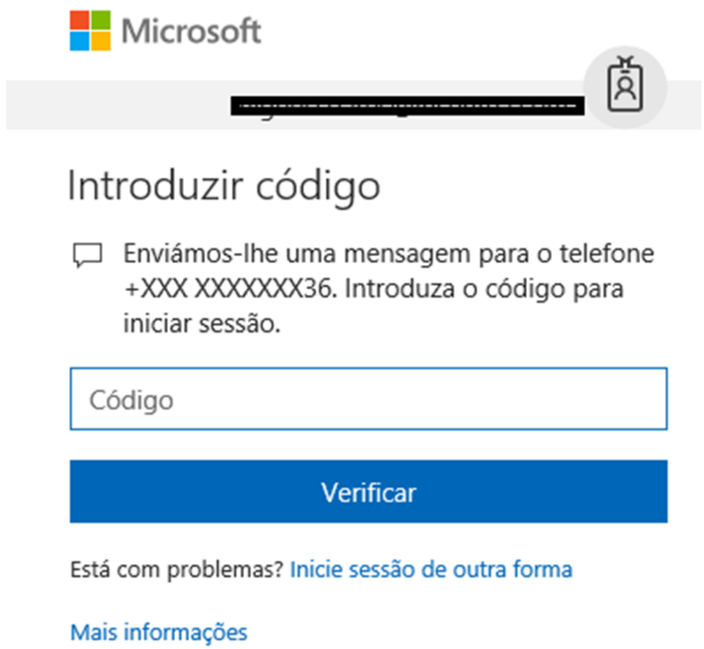
O esforço colocado na gestão e manutenção de um sistema deverá ser minimizado. Um único ponto de gestão com abrangência a toda a organização.

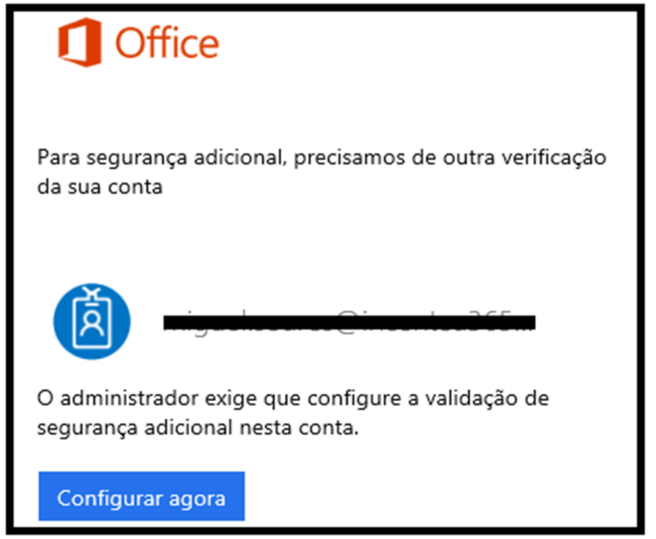
Exemplo 1 - Segurança Multifator - Email

Em quantos sites utilizo as mesmas password?

Cenário Real inCentea
MULTI-FACTOR AUTH

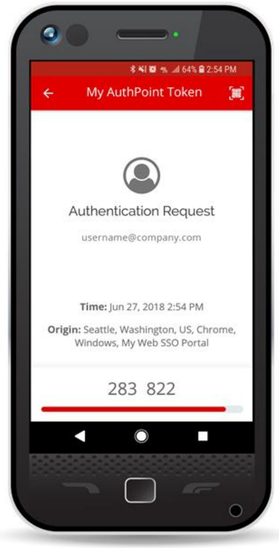
enabled vs enforced





Exemplo 2 - Segurança Multifator - VPN e Windows LogOn

O que acontece se a password for muito complexa?

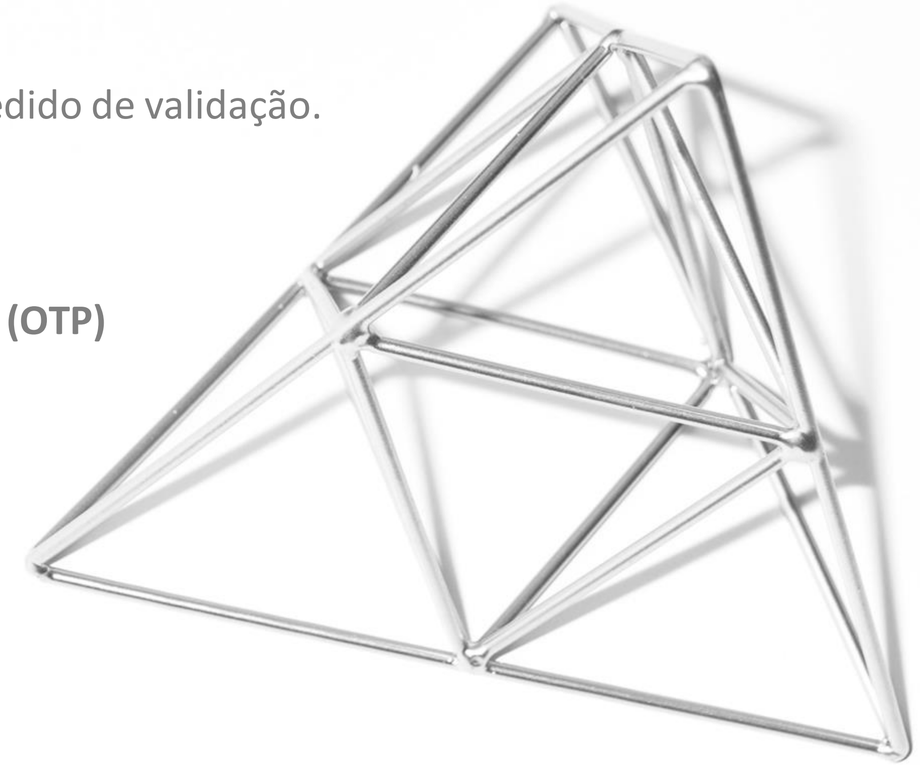


Watchguard Authpoint

(Não é necessário ter firewall Watchguard)

Ao estabelecer a ligação é feito o pedido de validação.

- **Push-Based Authentication**
- **Time-Based One-Time Password (OTP)**
- **QR Code-Based Authentication**



Exemplo 3 - Furto\Perca de Ativos

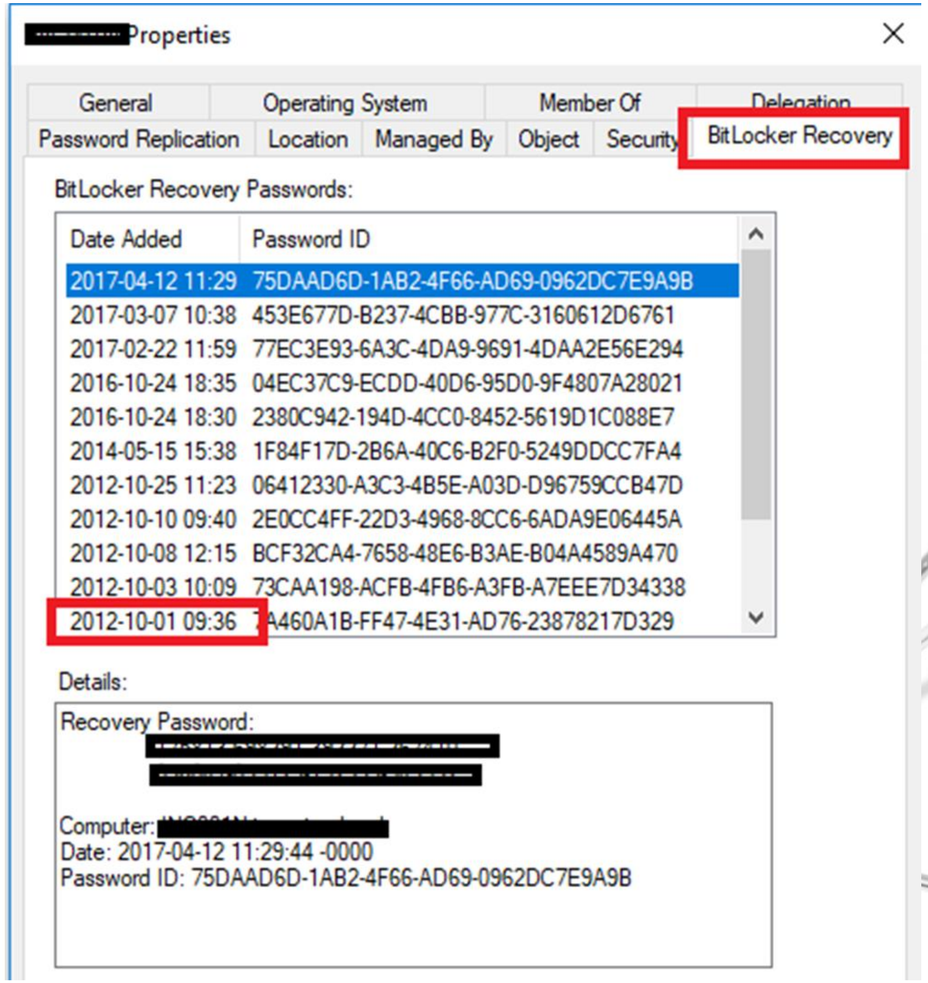
O Computador estava protegido com cifra **256-bit AES Encryption** ? (Bitlocker)

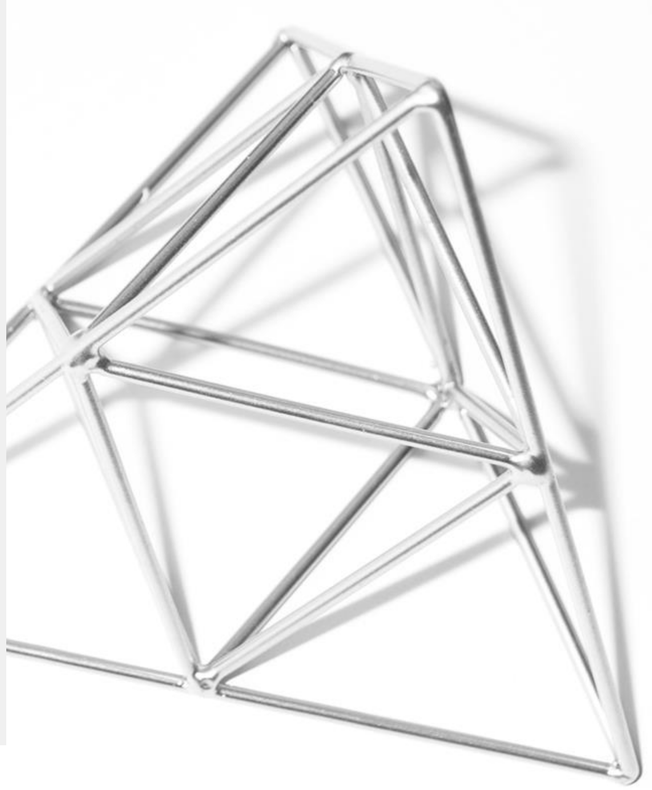
2 soluções:

- Bitlocker, com gestão na AD
- Sophos central Device Encryption

Sophos Central
Device Encryption

SOPHOS



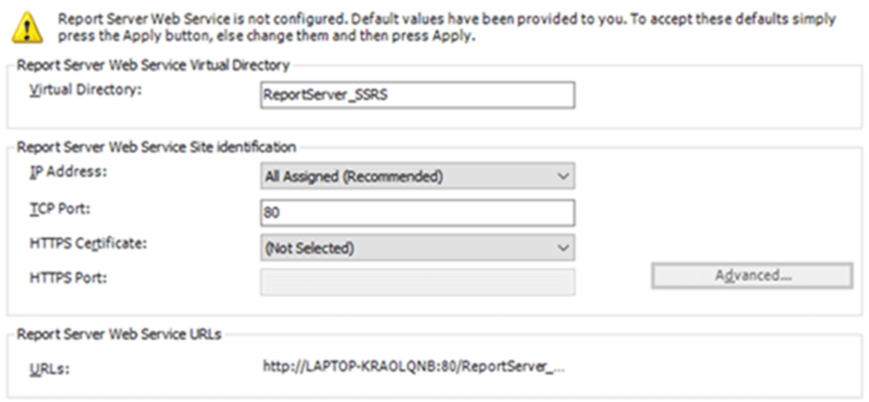


Exemplo 4 - Encriptação de Serviços WEB

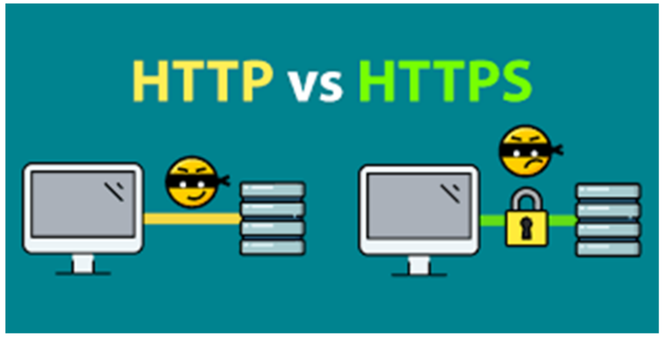
Informação em trânsito

Protocolos que não se devem usar:
SSL v2 - DROWN attack
SSL v3 - POODLE attack
TLS v1.0 - BEAST attack

Protocolos que se devem usar:
TLS v1.1 - okay
TLS v1.2 - suporta algorítmos criptográficos modernos



99% mal configurados?



Exemplo 5 - Controlo de dispositivos

O dispositivo que a conta foi configurada é autorizado?

inCentea Mobile Office 365 Policy

geral

▸ segurança

- [x] Exigir uma palavra-passe
- [x] Permitir palavras-passe simples
- [ ] Exigir uma palavra-passe alfanumérica

A palavra-passe tem de incluir esta quantidade de conjuntos de carateres:

3

- [x] Exigir encriptação no dispositivo
- [x] Tamanho mínimo de palavra-passe:
- [x] Número de falhas de início de sessão antes da eliminação de dados no dispositivo:
- [x] Exigir início de sessão após o dispositivo ter estado inativo durante (minutos):

minutos

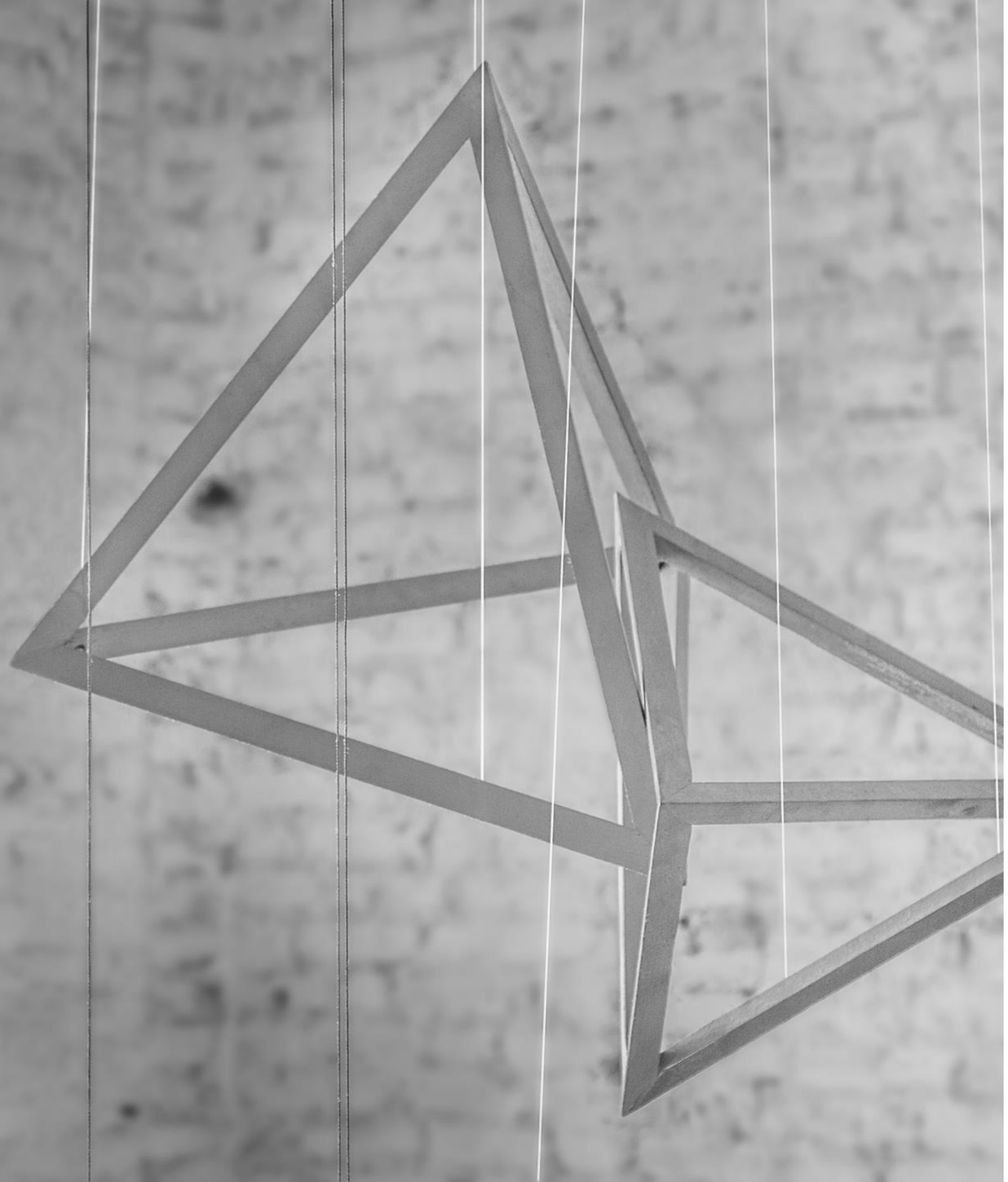
- [x] Impor duração da palavra-passe (dias):

dias

Contagem de reciclagem da palavra-passe:

2 soluções:

- Politica Office 365 (Exchange)
- Sophos Mobile Control



Questões

Servidores Seguros

Utilizar VPNs (segurança)

Politicas de segurança específicas

Controlar dispositivos que podem aceder

Postos de trabalho Seguros

Devem ter AV\solução Antiransomware

Controlo de acesso a sites

Passwords seguras

Multifator de autenticação

Encriptação do disco

Pessoas

"Firewall Humana"

Treino para identificar potenciais perigos

CASO 2
Proteção contra ameaças desconhecidas

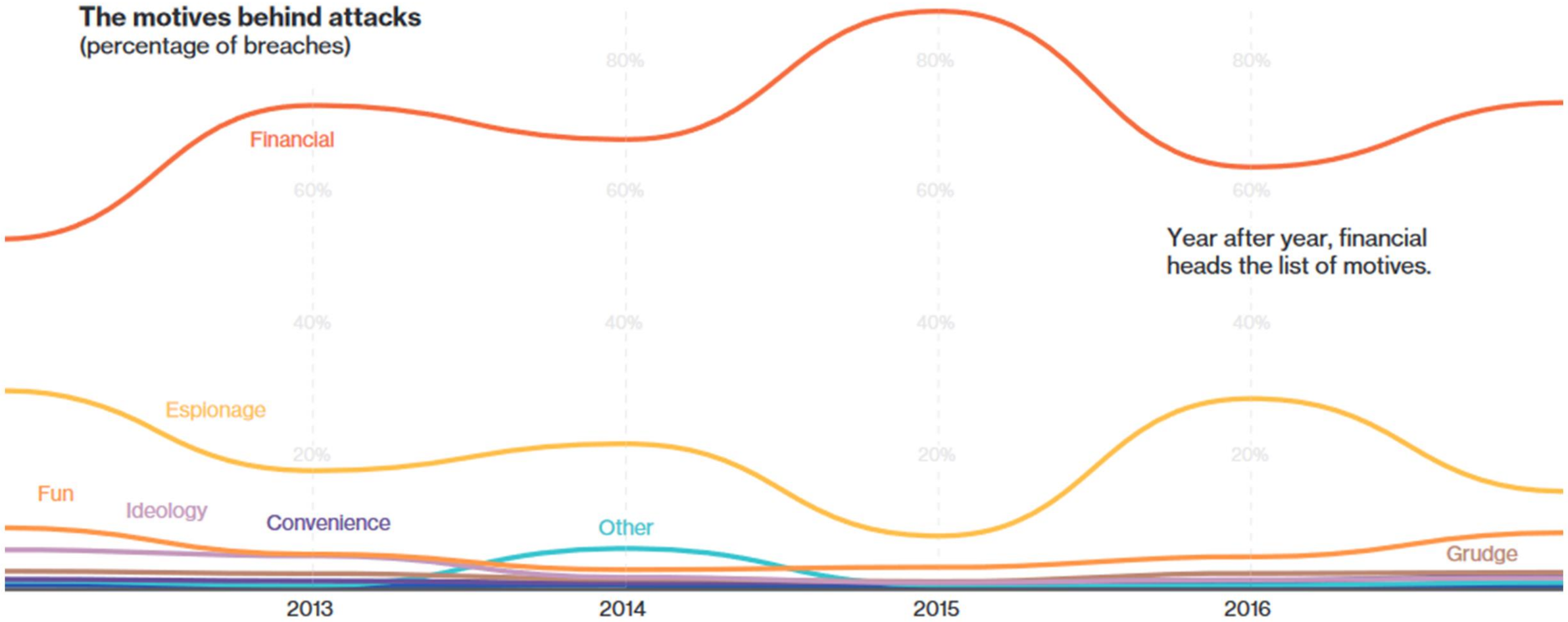
Segurança


SMBs are the primary targets for ransomware, but only 34% test backups regularly
30% of phishing emails are opened, and 12% of targets click on the link or attachment

INCIDENTES (violações) DE SEGURANÇA

Estudo 2018 Verizon

76% motivo financeiro. 73% ataques externos. 28% dos ataques envolveram colaboração interna.
!!!4% das pessoas clicam em qualquer campanha de phishing!!!
Ransomware continua a ser o top do software malicioso.

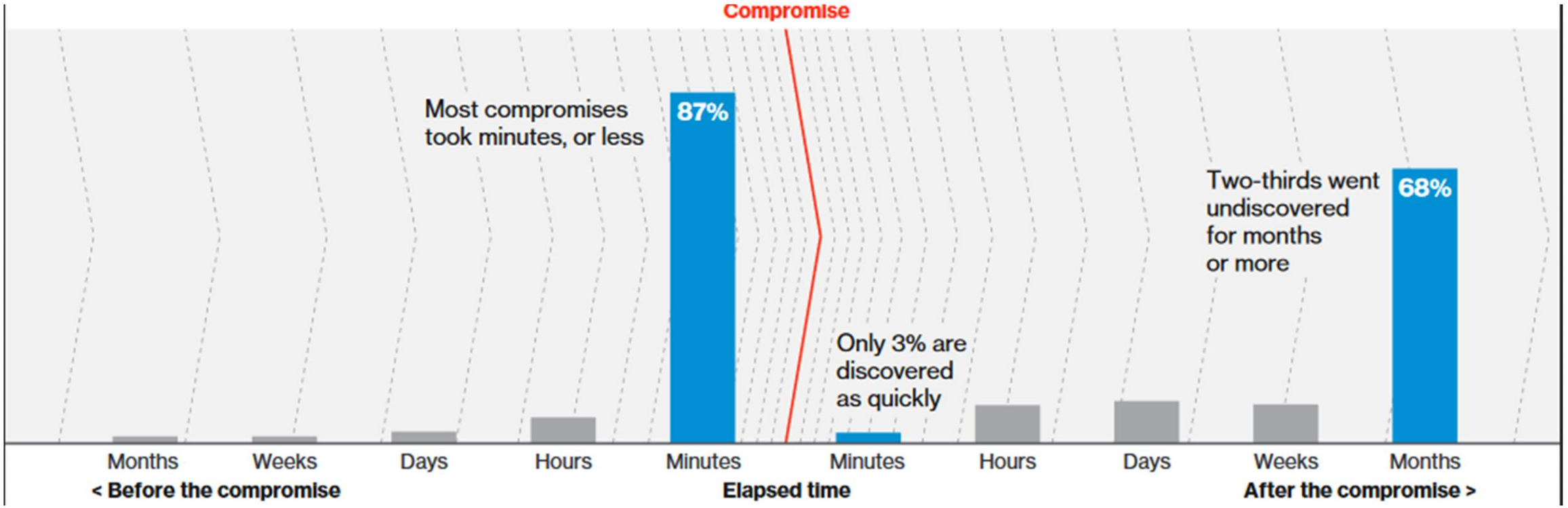


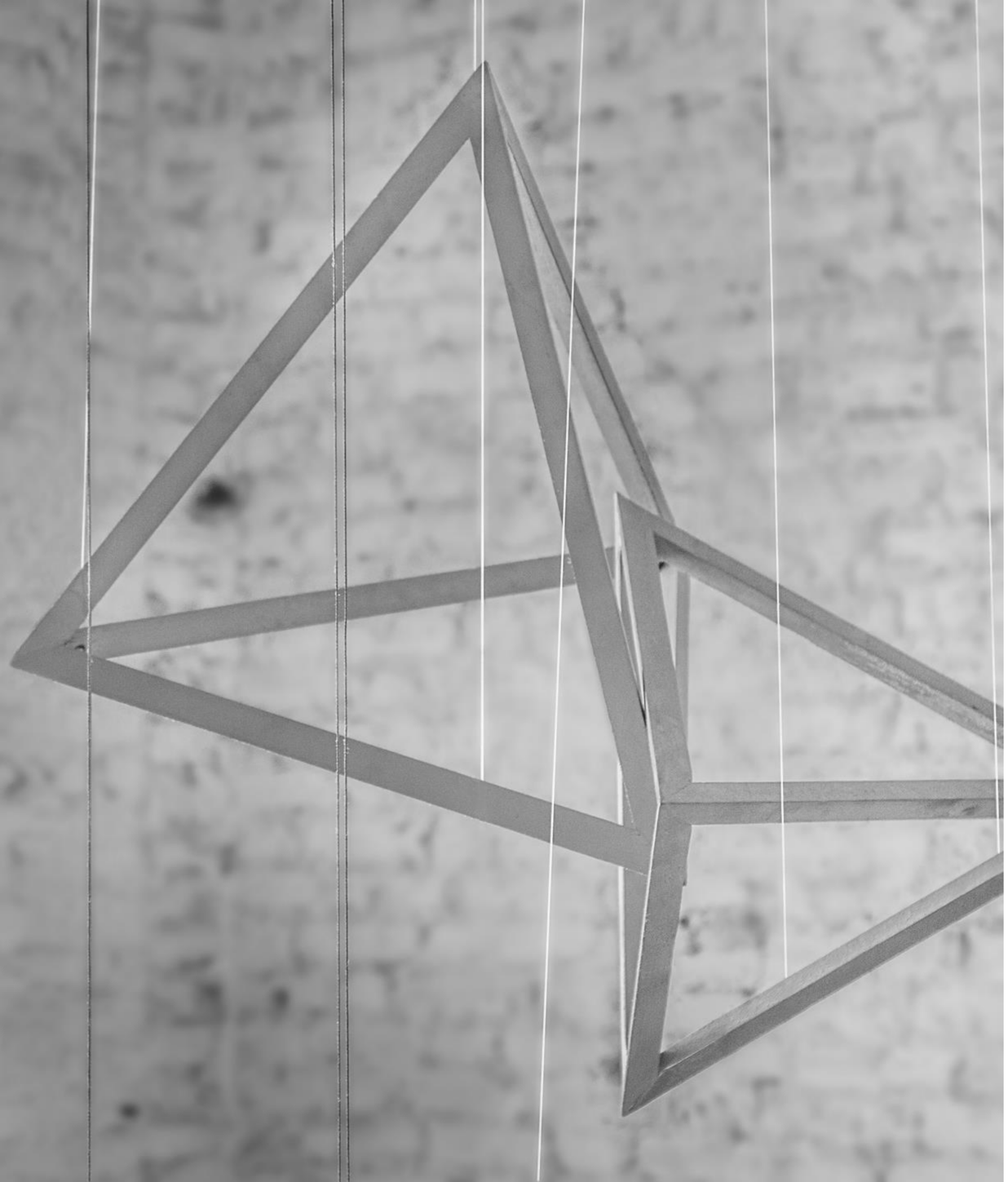
INCIDENTES (violações) DE SEGURANÇA

Estudo 2018 Verizon

68% das violações de segurança levam meses a serem descobertas.

Categorias: Aplicações Web, Uso errado de privilégios, furto ou perda de ativos, configurações erradas, erros humanos,…





Questões

Porquê

O Antivírus tradicional só funciona baseado em perigos conhecidos (vacinas)

O desconhecido necessita de outras técnicas de deteção

Funcionamento

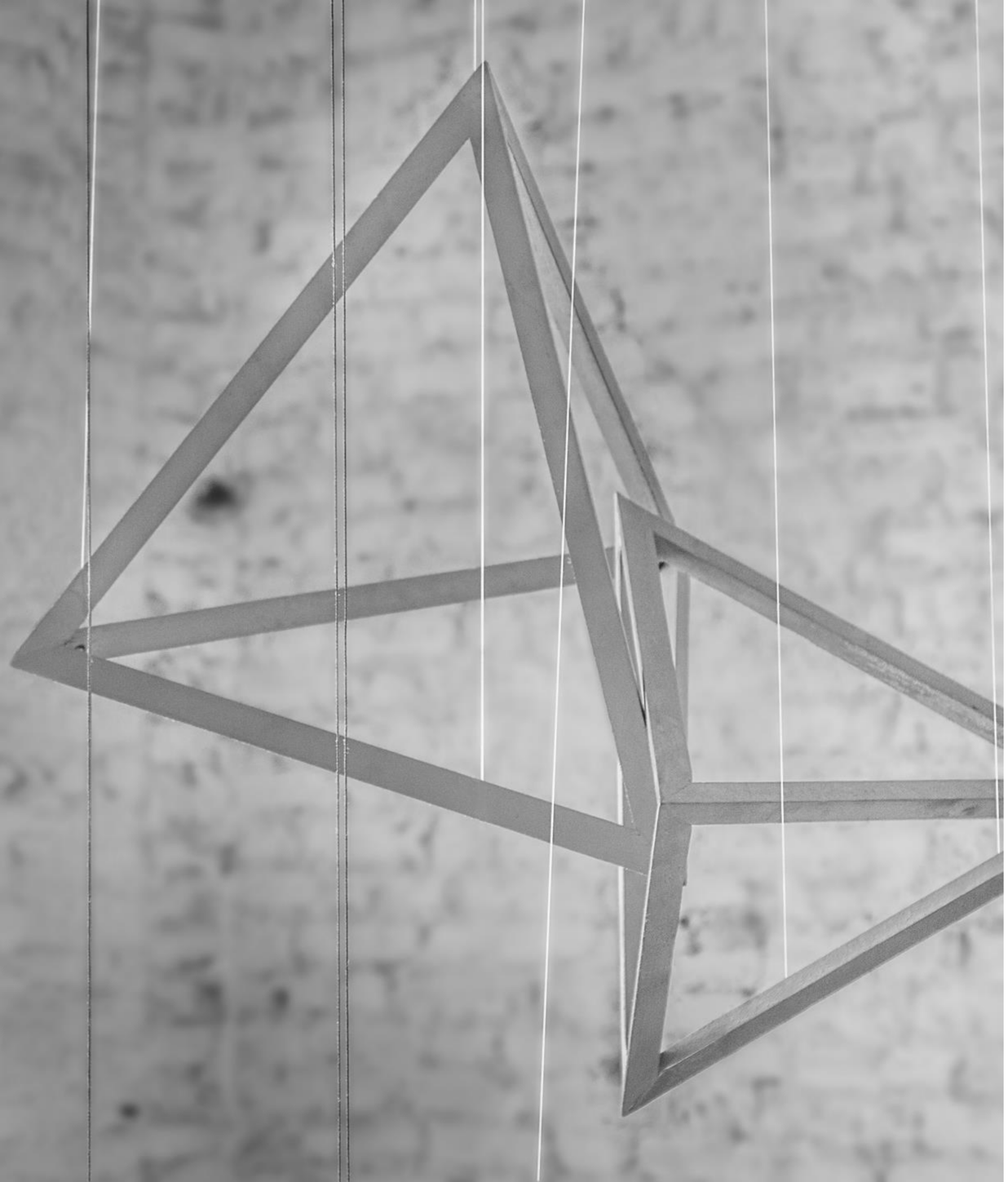
Vai detetar as ações executadas

(sintomas se doença - ex: COVID-19, em que não existe vacina)

Resultado

A principal função é o bloqueio do Ramsonware, mas os ataques podem ser direcionados com outros fins como roubo de informação

CASO 3
Instalar hardware sem intervenção física



Questões

Preparação

Ter conhecimento da infraestrutura do cliente (proximidade)
Fazer a inicialização antes de enviar\entregar o equipamento

Execução

Com a ajuda do cliente fazer a ligação física do equipamento
Caso seja necessário o cliente fornecer acesso remoto inicial
O tempo de implementação poderá ser um pouco superior

Resultado

Disponibilização do novo recurso\serviço na rede do cliente, evitando o contato presencial
Já foram realizadas diversas nestas últimas semanas:
- firewall; reinstalação servidor; PCs

CASO 4

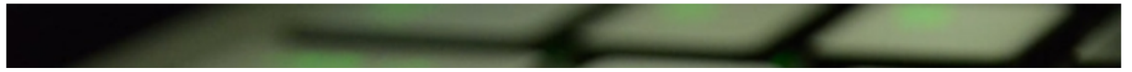
Pirataria em tempos de Covid19

Pirataria em tempos de Covid-19

Ataques informáticos aumentam em Portugal devido ao novo coronavírus

PJ relata várias campanhas de *phishing*, onde os piratas se fazem passar por outras entidades, como a Organização Mundial de Saúde.

Por TSF
17 Março, 2020 ▪ 21:11



Uma s

https://www.tsf.pt/portugal/sociedade/ataques-informaticos-aumentam-em-portugal-devido-ao-novo-coronavirus-11945277.html

CORONAVÍRUS

"Pandemia está a originar o maior volume de ciberataques que já vimos"

A maioria são ataques simples, mas com milhares a trabalhar de casa, e pouco tempo para formar os profissionais, a probabilidade de um computador "infectar" a rede é maior.

Karla Pequenino · 31 de Março de 2020, 6:58

https://www.publico.pt/2020/03/31/tecnologia/noticia/pandemia-originar-maior-volume-ciberataques-ja-vimos-1910028

Pirataria em tempos de Covid-19

ENERGIA

EDP foi alvo de ataque informático. Empresa garante que não há falhas no "fornecimento de energia"

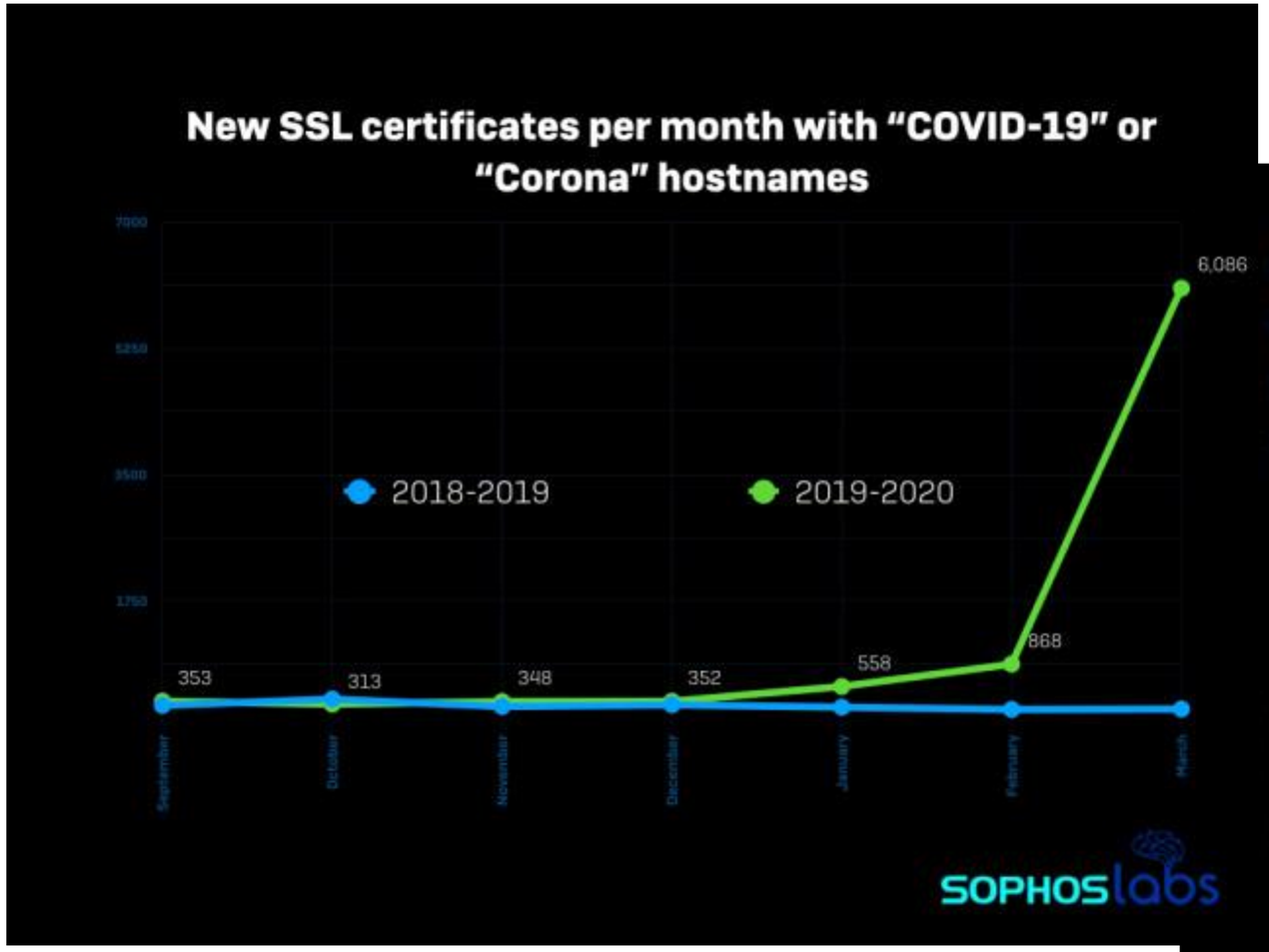
Empresa diz que o fornecimento de energia não foi afectado e que os serviços de controlo da rede eléctrica operam "normalmente, embora com adaptações".

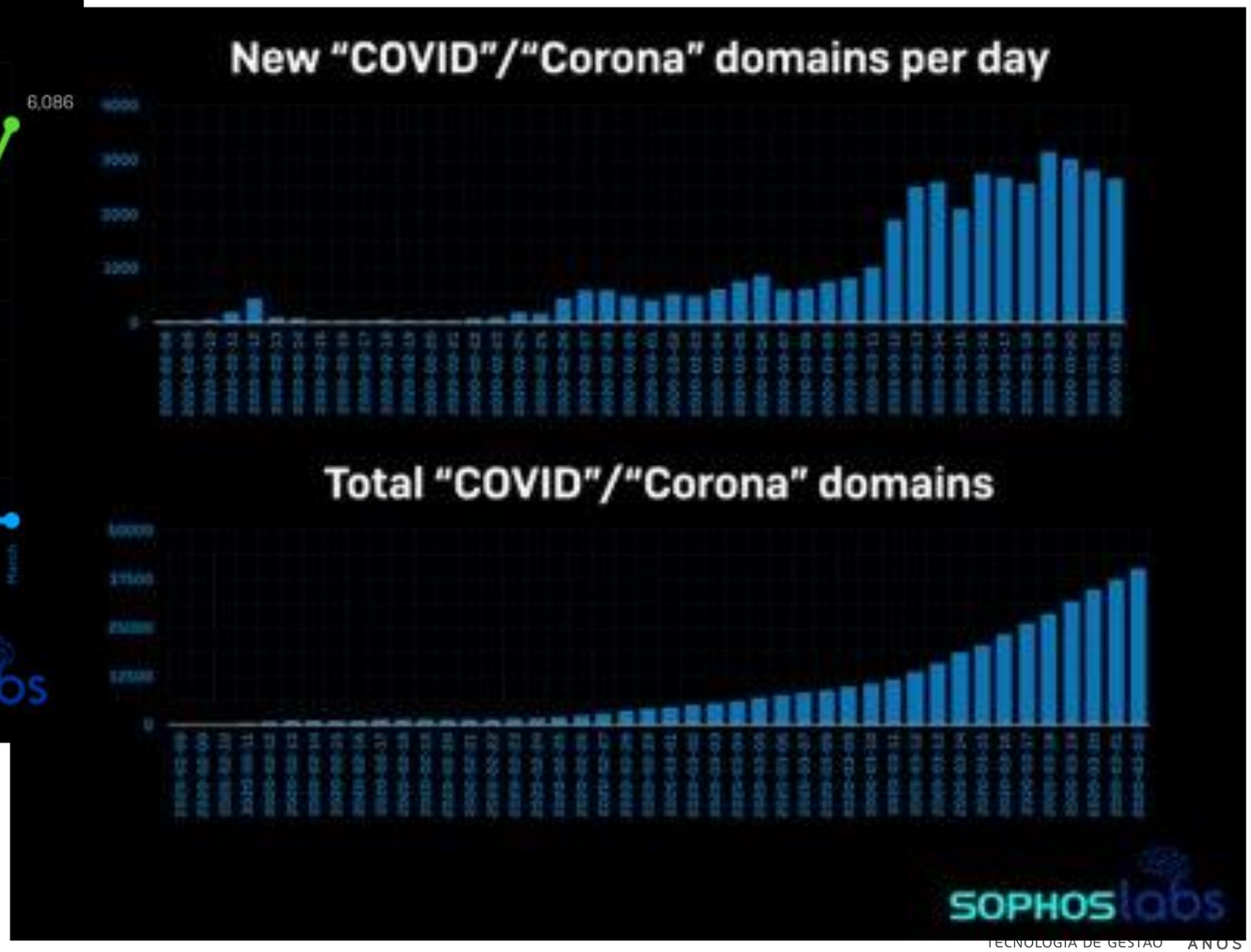
Ana Brito · 14 de Abril de 2020, 0:00

42 PARTILHAS

https://www.publico.pt/2020/04/14/economia/noticia/edp-alvo-ataque-informatico-empresa-garante-nao-ha-falhas-fornecimento-energia-1912186

1 - Pirataria em tempos de Covid-19





Pirataria em tempos de Covid-19

https://news.sophos.com/en-us/2020/03/24/covidmalware/

From: World Health Organization <donate@who.int>
Subject: COVID-19 Solidarity Response Fund for WHO - DONATE NOW
To: Undisclosed Recipients:

Reply | Reply All | Forward | More

5:57 PM

We are all affected by the growing COVID-19 pandemic. It's an unprecedented health challenge and we know people and organizations everywhere want to help. The World Health Organization is leading and coordinating the global effort, supporting countries to prevent, detect, and respond to the pandemic.

The greatest need right now is to help ensure all countries are prepared, especially those with the weakest health systems. **Donations support WHO's work to track and understand the spread of the virus; to ensure patients get the care they need and frontline workers get essential supplies and information; and to accelerate efforts to develop vaccines, tests, and treatments.**

Now you can help us by donating any amount you want with the help of BITCOIN NETWORK

DONATE NOW with Bitcoin payment

World Health Organization bitcoin address (BTC Wallet) for donations is: 39w2TUFxgyKNUipZBF54X3Dcf8Rv7zciLM

Your contribution will matter!

© 2020 WHO

World Health Organization

<cdworkscom@
March 27, 2020 at 9:15:10 AM EDT
To: <
COVID-19

Hi, neighbor.
Tests confirmed that I was sick with a coronavirus.
Doctors said that in the week I will leave the world.
My parents will be left without my support.
And at this time you will live enjoying.
I think this is unfair, and I suggest you pay me.
What I am sitting at home and don't try to infect your home.
Life or money.
Hurry up! Every hour, I hate you more and more.

My bitcoin address (BTC Wallet)

SOPHOSlabs

Burla e Falsidade Informática por e-mail

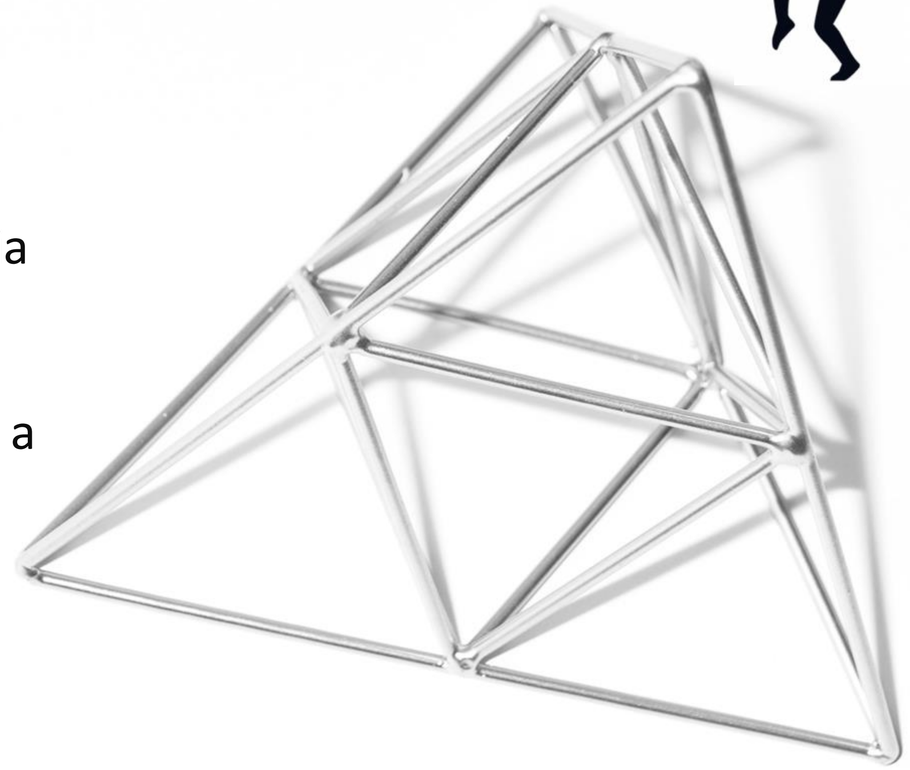
1. Vitima viajou recentemente e/ou acedeu a redes wireless inseguras para consultar o email profissional

2. As credenciais da vitima são interceptadas de forma “silenciosa”, a vitima não se apercebe de que as suas credenciais foram roubadas

3. O Hacker monitoriza a troca de emails à espera de um pedido de pagamento para um determinado IBAN legitimo.

4. Assim que o hacker deteta o numero IBAN numa mensagem, recria uma réplica da mensagem original com um IBAN diferente.

5. A semelhança das mensagens é de tal forma bem conseguida que a vitima nunca se apercebe que está a responder a um remetente diferente.



https://www.policiajudiciaria.pt/burla-e-falsidade-informatica-em-transacoes-empresariais-transnacionais/

Descubra as diferenças

qua 11/03/2020 11:04

[redacted]e@flui[redacted]

I: EXPIRED INVOICES - [redacted] (OC 1913.19 REF Order ENF 1901374 + OC 1909.19 - Inv. 2/91)

Para [redacted]

Respondeu a esta mensagem em 11/03/2020 12:03.

bank details Banca di San Marino.pdf
119 KB

Itens de ação + Obter ma

Dear S[redacted],
Good morning.

I wrote several times whitout answer by your side.

I need to received with urgency the payment of the overdue invoices.
Please answer me.

Regards.

[redacted]

Accounts & Administration Department

[redacted]

ISO 9001:2015

sex 13/03/2020 08:49

[redacted]e@fliu[redacted]

R: EXPIRED INVOICES - [redacted] (OC 1913.19 REF Order ENF 1901374 + OC 1909.19 - Inv. 2/91)

Para [redacted]

Cc [redacted]

Respondeu a esta mensagem em 16/03/2020 11:08.
Se existirem problemas com a forma como esta mensagem é apresentada, clique aqui para vê-la num browser.
Clique aqui para transferir imagens. Para ajudar a proteger a sua privacidade, o Outlook impediu a transferência automática de algumas imagens desta mensagem.

Dear S[redacted],
Please our bank details has changed. **Do not pay to former account anymore.**
How many euro are you paying?
Let me know, please so I can send our NEW BANK ACCOUNT.
Waiting your response.

Kind regards.

[redacted]

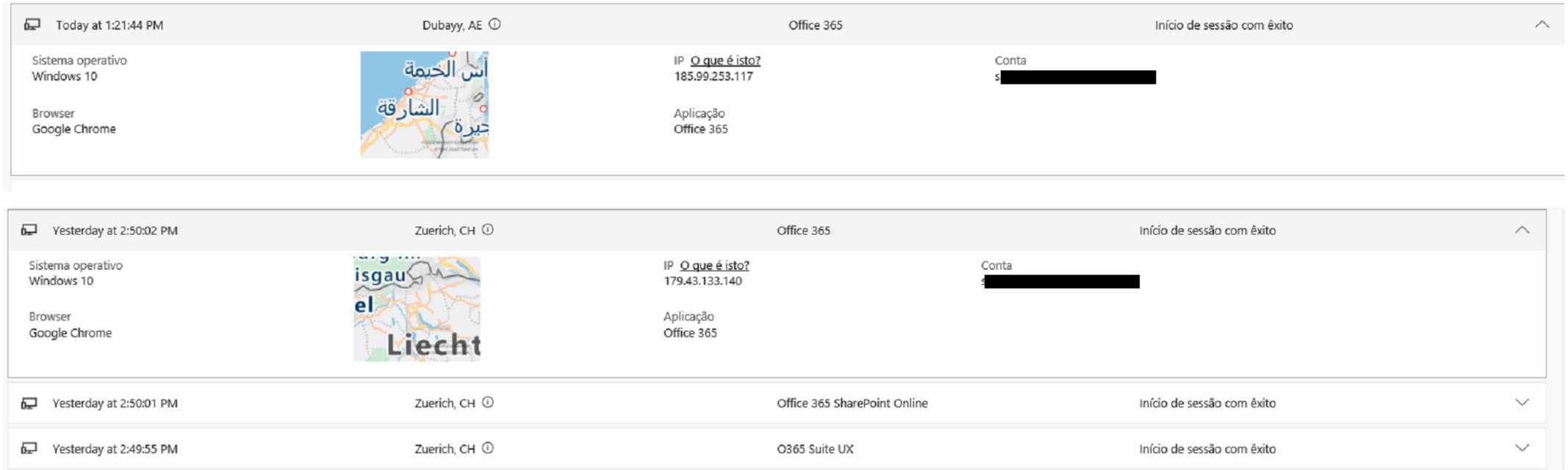
Accounts & Administration Department

[redacted]

ISO 9001:2015

Prevenção

1. Monitorizar acessos ao email



2. Preservar uma politica de palavras-passe segura

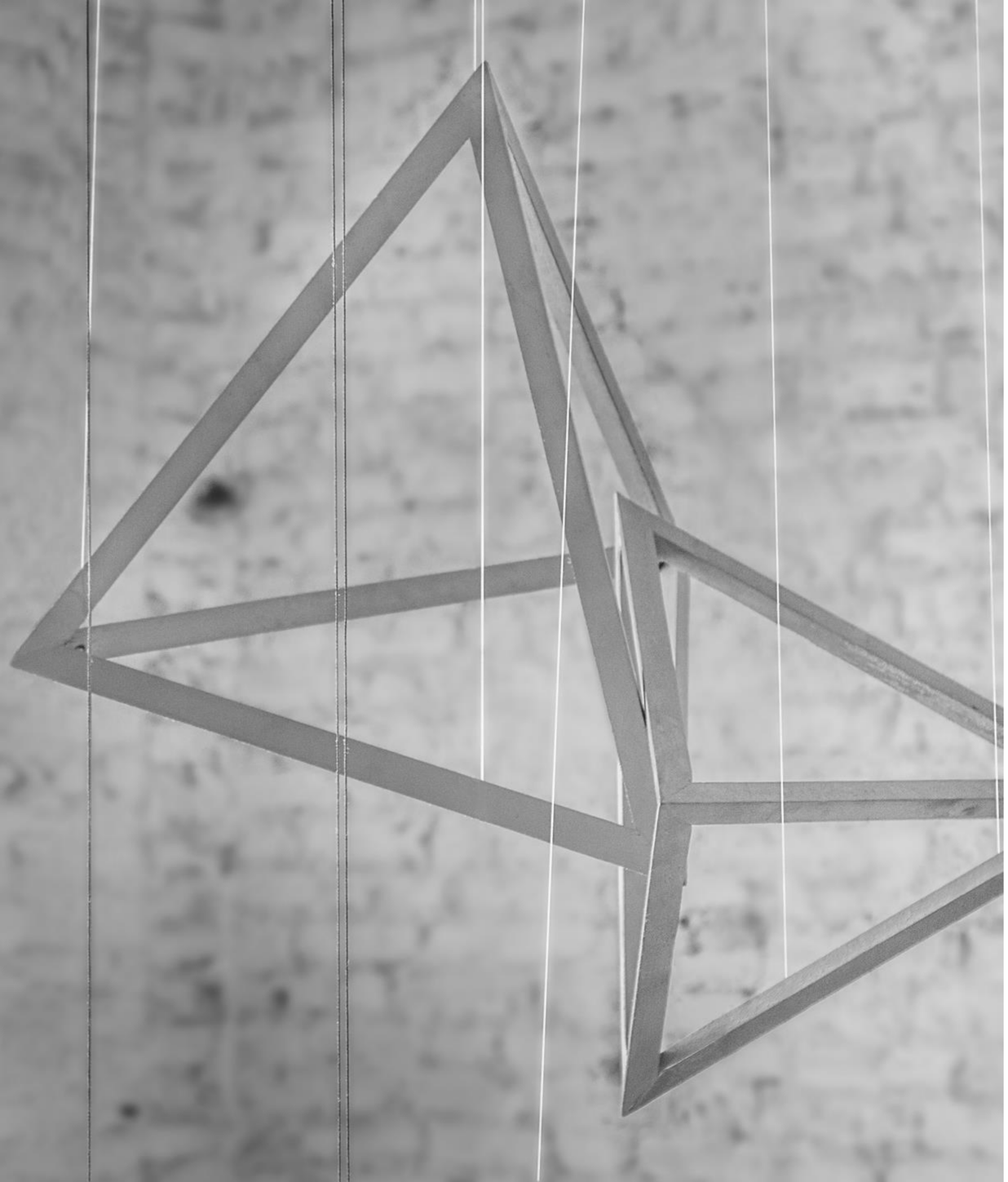
3. Ativar segurança adicional de autenticação multifator (MFA)

4. Observar sempre o endereço de email para quem estamos a responder

5. Não utilizar o mesmo computador para finalidades profissionais e pessoais

CASO 5

As aplicações Cloud não precisam de manutenção e são 100% seguras?



Questões

Manutenção

Depende:

- Nas plataformas SAS, a manutenção é encargo do fornecedor do serviço
- Nas plataformas IAS, o cliente é responsável pela sua manutenção

Segurança

Nada é 100% seguro

Só por existir uma firewall ou backups o cliente não está protegido

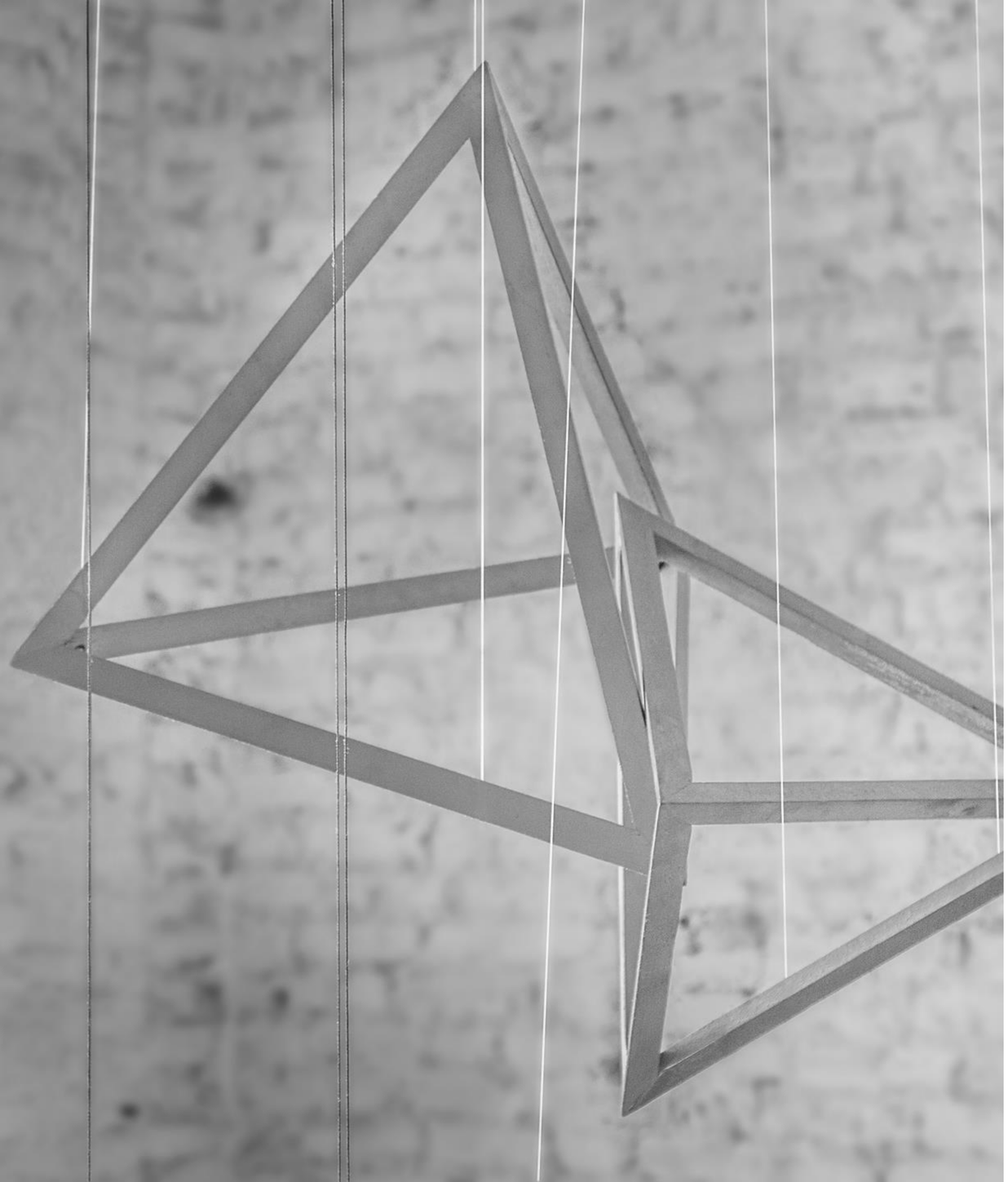
Existem muitos fatores que afetam a segurança, deve ser feita uma análise e mitigar os principais

Resultado

Os clientes ao migrarem as aplicações para a Cloud não podem deixar de ter preocupações de segurança.

Essas preocupações passam a ser diferentes

Ex: (Ambientais vs todas as outras)



Parceiro oficial certificado de várias marcas do mercado

Alcatel·Lucent Enterprise
Accredited Business Partner

WatchGuard ONE | Gold Partner

Hewlett Packard Enterprise
Solution Provider
Hybrid IT
SILVER PARTNER

Sophos Platinum Partner

Gold Microsoft Partner
Microsoft

vmware PARTNER
PROFESSIONAL SOLUTION PROVIDER

VEEAM PRO PARTNER
SILVER RESELLER

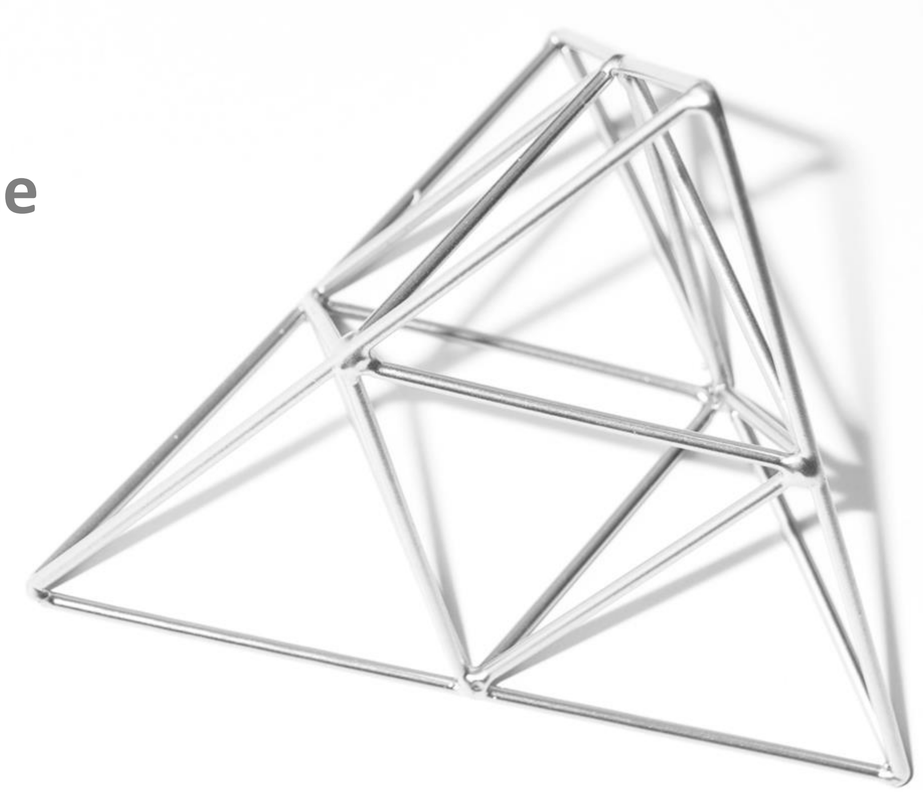
StorageCraft gold partner

APC by Schneider Electric
PREMIER PARTNER

Próximos Webinares

22 Abril **11h** **Serviços Geridos**

29 Abril **11h** **Segurança - soluções ao detalhe**



Obrigado

WWW.INCENTEA.COM

PESSOAS COM SOLUÇÕES

inCentea TECNOLOGIA DE GESTÃO 30 ANOS


PESSOAS
COM
SOLUÇÕES