P2T: Um Sistema de Correio Eletrónico com responsabilidade orientada para o utilizador remetente

António Pais
antonio.pais.p2t@p2t.email
https://p2t.email

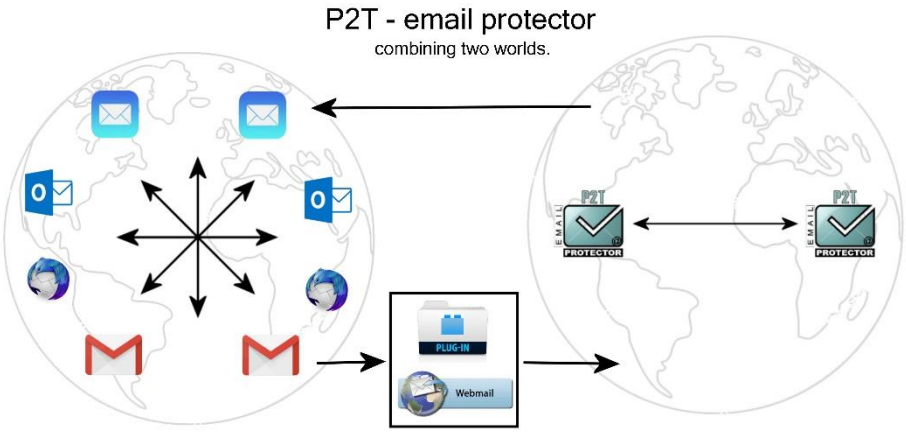
Sinopse. O serviço de correio eletrónico está assente numa estrutura de protocolos de comunicações cliente-servidor criada em 1971 e desde então o seu principal objetivo foi sempre o envio livre e direto de mensagens de um remetente para um ou mais destinatários sendo apenas exigido saber os endereços de email. Devido à rápida adoção que tomou, as necessidades de segurança para os anos que se seguiram foram negligenciadas a nível de nova estrutura optando-se apenas por se criar camadas externas de soluções para continuar a manter o requisito básico a que se propôs desde a sua criação. Hoje e apesar de toda uma tecnologia a crescer de forma exponencial associada a grandes players cujas ferramentas prometem capacidades de proteção em 99,99%, ainda assim ao fim de 50 anos considera-se o email como o maior vetor de ataque para ransomware, phishing e malware em geral. Propõe-se a criação de um novo software de servidor de correio eletrónico a correr numa rede constituída por um consórcio de provedores de serviços de email com características anti-spam, através de um modelo chamado de "Controlo de Fluxo por seleção" (FCbyS) e que vai funcionar numa perspetiva de responsabilidade orientada para o utilizador remetente, removendo assim a necessidade de investimento em tempo, recursos humanos e tecnologia avançada para resolver um problema criado por terceiros. A estrutura será assegurada por um modelo de consenso DAO (Organização Autónoma Descentralizada) de forma a permitir os constantes melhoramentos da rede e do software servidor tanto na fase de implementação de novos requisitos como na segurança dos seus constituintes.
A compatibilidade com os utilizadores tradicionais será assegurada por meio de um gateway que alem do seu modo nativo, vai fornecer mais duas alternativas de comunicações sem a necessidade de alteração dos protocolos de email conhecidos.

1. Introdução

Este whitepaper descreve os métodos aplicados na proposta do P2T- email Protector para proteger os utilizadores contra spam de email usando um novo conceito chamado pelo autor de "Flow Control by Selection (FCbyS)". Esta abordagem inovadora permite que os destinatários de mensagens de email eliminem os custos associados a comprometimentos de segurança criados por terceiros. Os serviços de email são o mecanismo número um de distribuição de malware e cibercrime a nível global, diz David Bennett, diretor de operações da Defense Information Systems Agency, e especialista de cibersegurança do Departamento de Defesa dos Estados Unidos. O cibercrime está a caminho de ultrapassar 10.5 mil milhões de dólares a nível global até ao ano de 2025. Este tipo de mercado já é superior ao atual mercado negro mundial de moeda falsa e drogas ilegais combinadas. De acordo com o FBI, o phishing foi o tipo mais comum de crime

cibernético em 2020 (96%) e os incidentes de phishing quase dobraram de frequência, de 114.702 incidentes em 2019 para 241.324 incidentes em 2020. As reclamações foram superiores a mais de 11 vezes em 2020 em comparação a 2016. Todo o volume de spam mundial já é de 75% sendo responsável por ransomware, phishing e outros tipos diferentes de malware fazendo deste tipo de atividade criminosa como o vetor de ataque preferido. Para resolver esse problema, criamos uma estrutura nova e paralela com regras específicas e proactivas. O P2T - Email Protector, liberta a tecnologia e recursos financeiros para outras tarefas mais importantes e aos utilizadores de preocupações com spam de email por uma fração do preço das outras ofertas de mercado.

O diagrama a seguir mostra o posicionamento de mercado



P2T a usar o novo modelo de proteção: Flow Control by Selection (FCbyS)

2. O panorama do email; Atuais Desafios

Nos últimos anos, a qualidade dos ataques cibernéticos, especialmente via email, tornou-se sofisticada, com os cibercriminosos encontrando maneiras criativas de contornar os controles de segurança e o comportamento humano. Eles mudam constantemente seus métodos e meios de ataque, dificultando a deteção e criando métodos facilitadores para que o utilizador desista de algo valioso. Os invasores também começaram a segmentar pessoas de todos os níveis da organização, os seus clientes e até parceiros. Basta visitar um site comprometido e é tudo o que é necessário para criar prejuízos não apenas no seu computador, mas também nas partilhas associadas à sua conta. Esses ataques geralmente são enviados por meio de emails fraudulentos que parecem vir de um remetente legítimo. Porque é que o atual modelo de proteção não resolve o problema do spam de email?! Porque ele usa FILTROS (alguns mais complexos que outros, como filtrar conteúdo para reputação de IP, usar métodos heurísticos, listas brancas, listas negras, listas cinzas, etc.), e estes modelos de filtragem são modelos reativos, são paliativos, inadequados, porque se tornam rapidamente obsoletos pela espantosa tecnologia de spam e botnet que aumenta exponencialmente quase todos os dias. Por esta razão, várias empresas sentiram a necessidade de procurar alternativas (Skype, WhatsApp, Slack, Microsoft Teams, Telegram…) ainda que menos produtivas, mas mais seguras para substituir os meios cada vez mais permissivos de abuso. Até agora, todas as alternativas encontradas funcionam bem entre os seus pares, restringindo a comunicação entre diferentes participantes do mercado. Mas o email ainda é o melhor serviço de comunicações no local de trabalho em grandes e pequenas empresas, com um funcionário a enviar 40 e a receber 121 emails em média por dia. Também verificamos todos os

dias a necessidade de usar um endereço de email nos mais variados serviços da Internet. Portanto, não é surpresa que o email continue sendo a ameaça de segurança mais explorada numa organização. O P2T - Email Protector tem um papel fundamental para fornecer aos utilizadores um canal de comunicação seguro com todos os intervenientes do mercado.

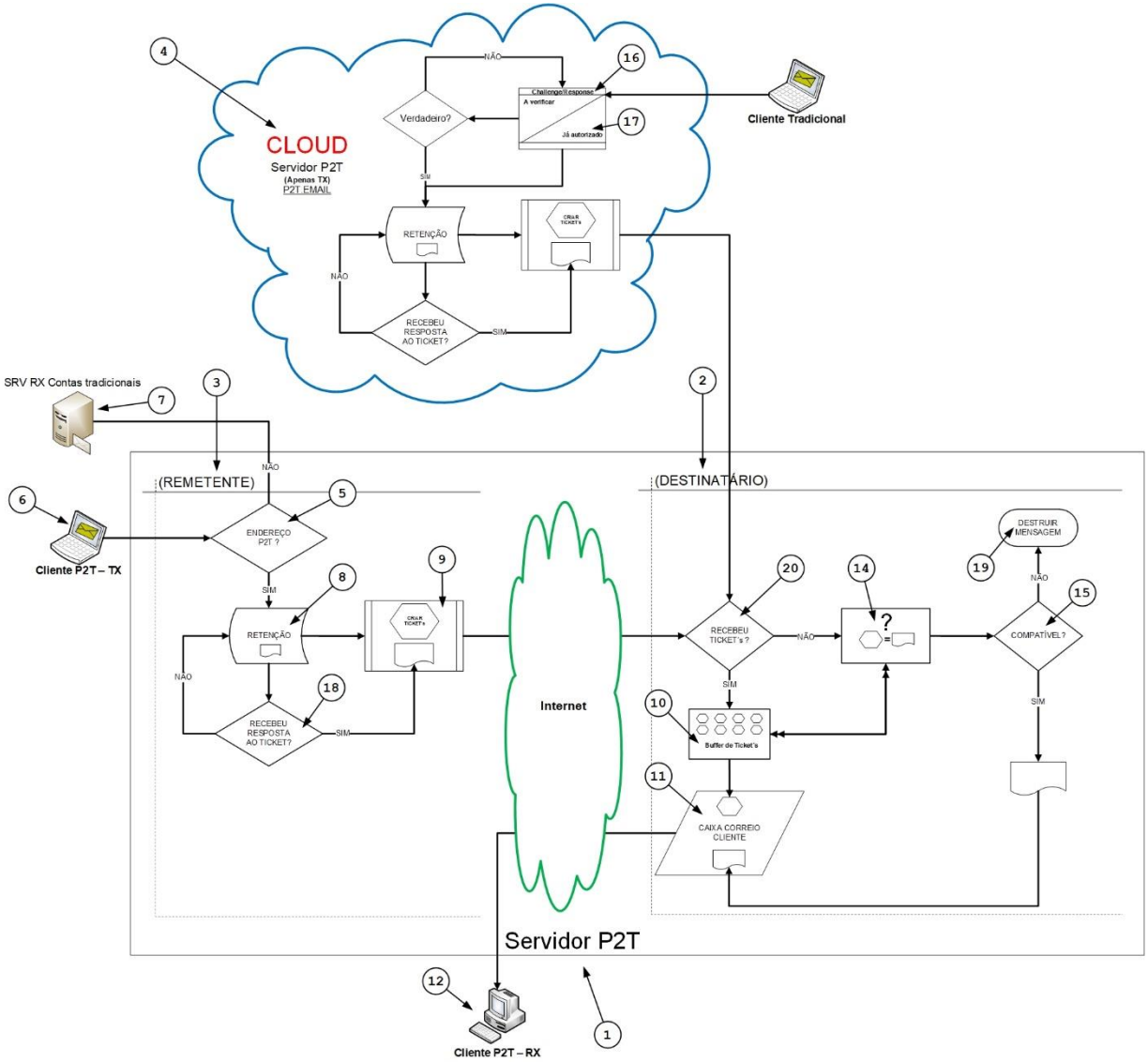
3. Procedimentos padrão

Como o nível de sofisticação e o volume de ataques a emails aumentará no futuro, somente pensando além da defesa reativa e abordando a segurança de email de maneira mais ágil, as organizações podem impedir ameaças de email tanto na segurança interna quanto a externa. A nova categoria de proteção do P2T - Email Protector usa um modelo preventivo e eficaz, agindo diretamente na fonte de spam.

Adaptação ao cliente

Adotar uma nova solução significa enfrentar a ansiedade e a inércia de velhos hábitos. Os clientes só passam por isso quando a sua solução fornecer um valor suficientemente importante. É por isso que editar um email, enviá-lo e recebê-lo terá um impacto mínimo no seu comportamento regular. A pasta de spam é eliminada e a pasta de envio pode ser gerida e personalizada. Esta é a única mudança de regra estrutural. Gerindo a caixa de saída, em vez da caixa de entrada, como é habitual numa configuração tradicional.

Anatomia da Ferramenta



Criação de um novo servidor de email com recursos internos de gestão de email mais produtivos.

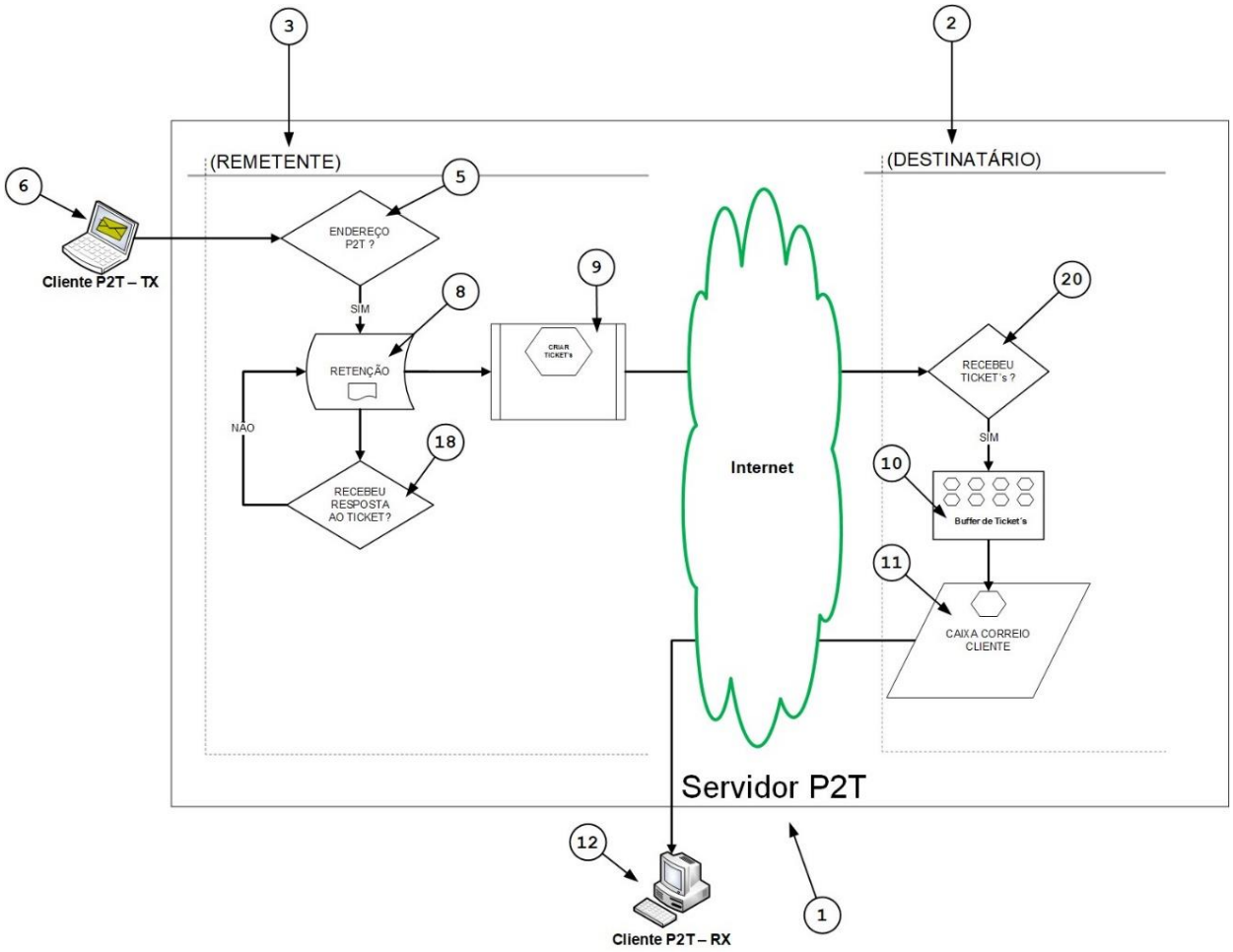
a) A responsabilidade de gestão do email muda do destinatário para o remetente.
b) O servidor destinatário realiza um processo de seleção, onde receberá apenas dois tipos de dados.
   - Notificações
   - Mensagens precedidas por notificações
c) Desenvolvimento de um gateway em nuvem para garantir a compatibilidade.
d) Criar um "plug-in" para dar suporte à comunicação.
e) Todos os servidores serão executados em software proprietário controlado pelo consórcio.

4. Comunidade de Membros. Como funciona P2T (FCbyS)

Três cenários possíveis:

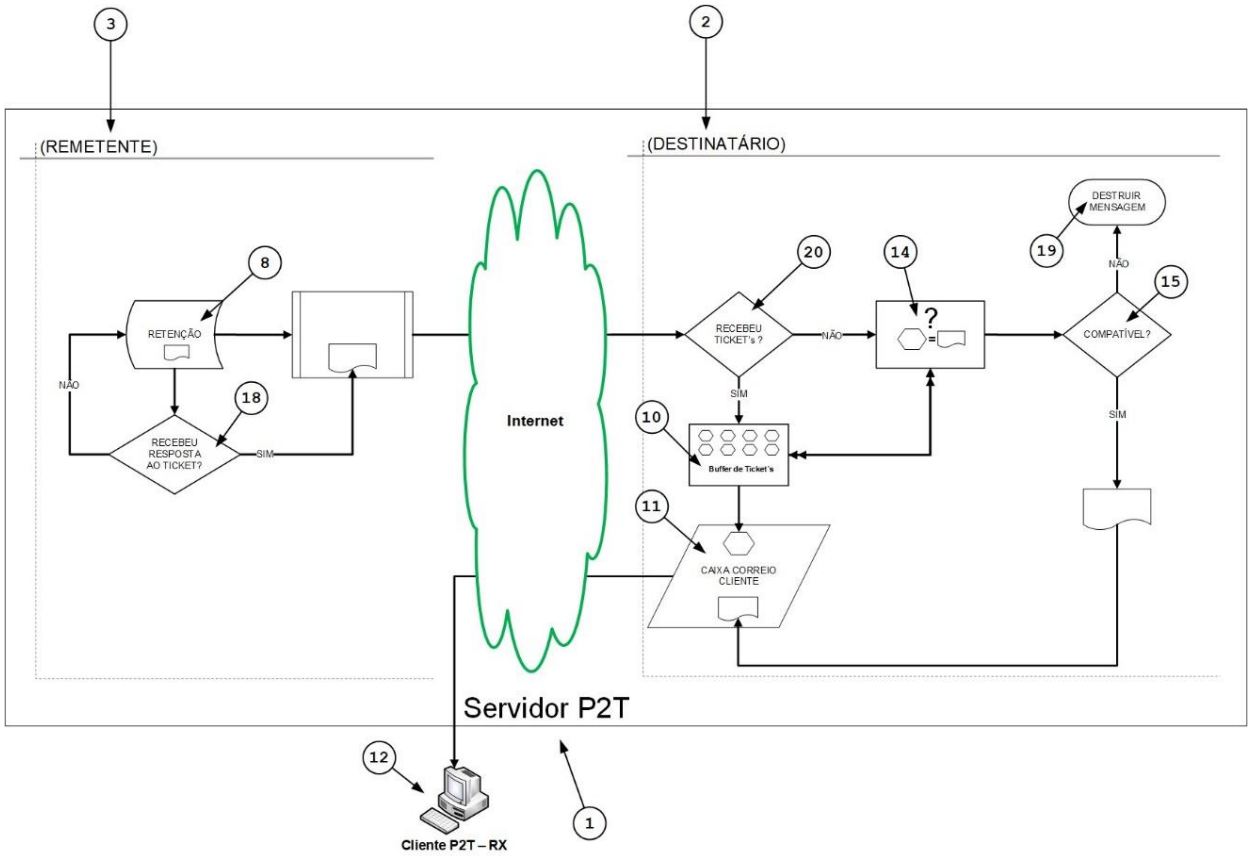
1. Envio de emails entre utilizadores P2T

   Processo de envio.



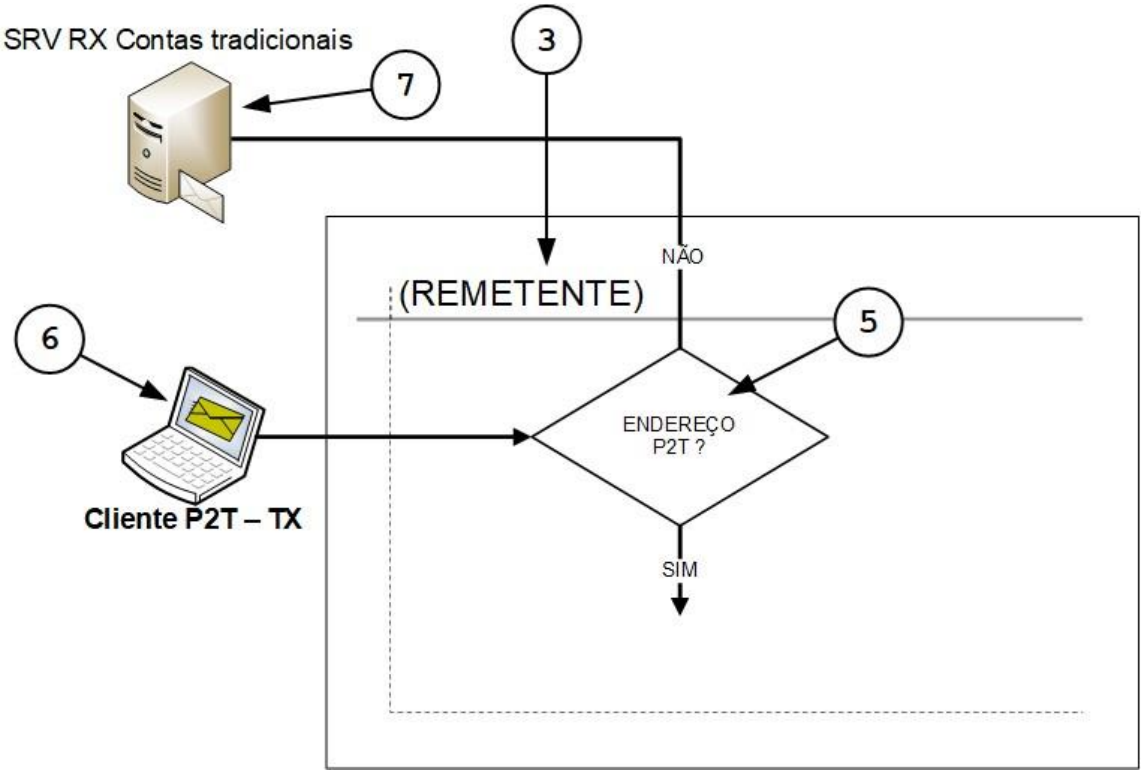
--

Processo de receção.



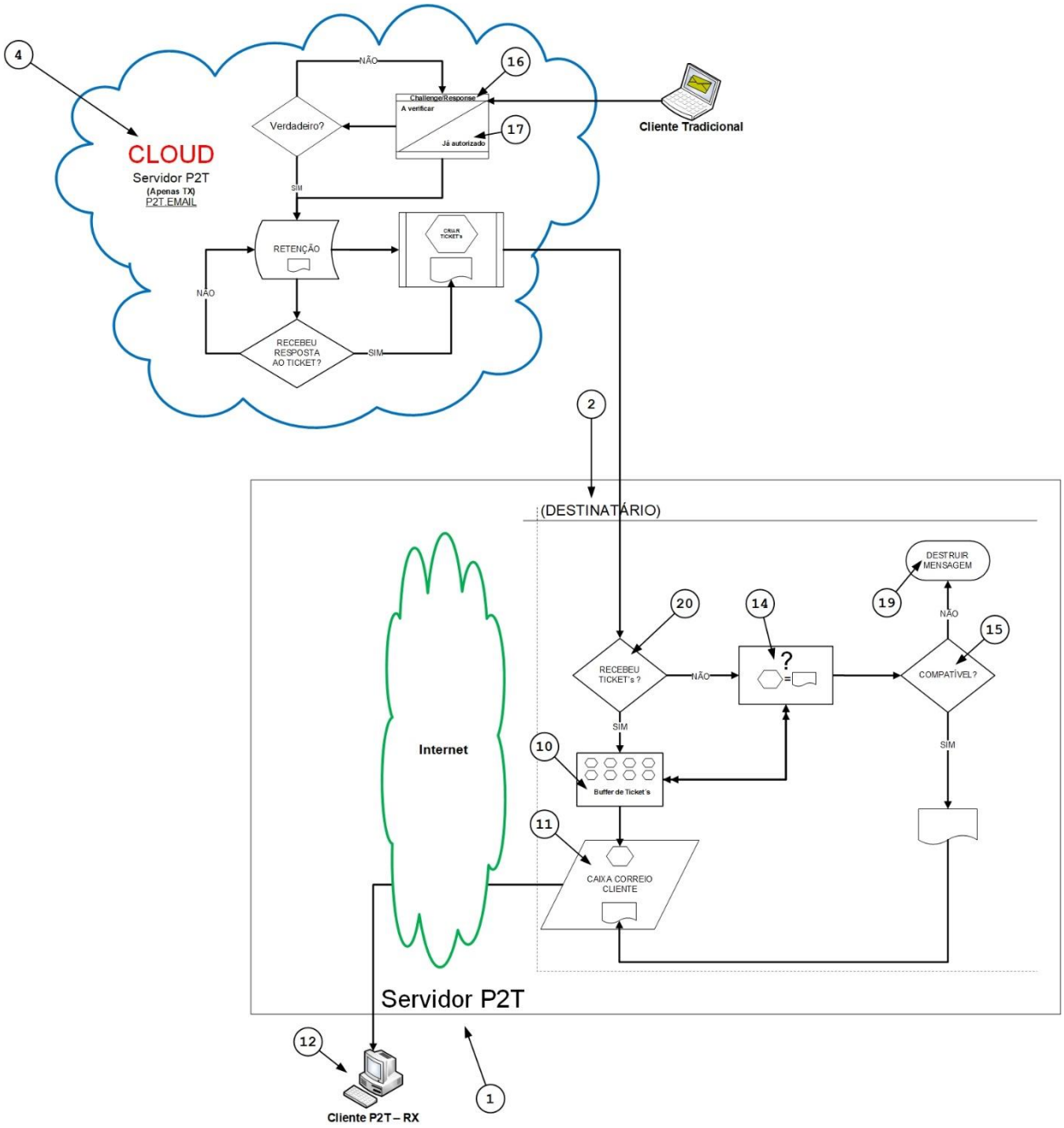
Todas as mensagens enviadas são retidas no servidor do remetente. Na sua vez, será enviada uma notificação (com a identificação do remetente e do destinatário, o assunto, a data e hora de receção, informações de anexos e um botão Ignorar/Aceitar) para a caixa de entrada do destinatário (INBOX). Todas as mensagens retidas na caixa de saída do remetente (OUTBOX) serão libertadas somente quando o destinatário clicar no botão "Aceitar" da notificação. Lidar com todo o "lixo de mensagens" e capacidade de armazenamento do servidor é, a partir de agora, um problema do remetente.

2. Envio de mensagens para utilizadores tradicionais



Neste cenário não há inovação. Este processo utiliza os atuais protocolos de comunicação SMTP correspondentes a todos os participantes da rede. A mensagem do utilizador P2T vai diretamente para a caixa de entrada do destinatário tradicional.

3. Receber emails de utilizadores tradicionais



O P2T - Email Protector desempenha um papel fundamental de forma a fornecer aos utilizadores um canal de comunicação seguro com todos os participantes da rede. Para todos os clientes que possuírem um livro de endereços confiável do cliente P2T, um "plug-in" gratuito será automaticamente concedido. Ao instalar o plug-in no seu fornecedor de email habitual, os utilizadores tradicionais tornaram-se compatíveis com o P2T. Esse recurso permite que os utilizadores P2T permaneçam protegidos enquanto recebem comunicações de utilizadores tradicionais. A outra forma dos utilizadores tradicionais se manterem em contato com utilizadores P2T é através de um serviço de webmail disponível numa página web.

O cliente P2T terá o acrónimo "p2t" que precede o símbolo de email "@"; exemplo: nome.p2t@dominio. Essa automatização será criada por meio de um "alias".

5. Pontos chave

Ferramentas inovadoras de proteção;

- Ocultação de identidade.

O modelo tradicional de email facilita o uso de uma identidade falsa dificultando o rastreamento. No caso do utilizador tradicional, o destinatário do email não tem escolha, a mensagem já está na caixa de entrada (INBOX).

Quão grave é este problema? Numa pesquisa da Tessian, empresa de software de segurança de email para o mercado empresarial, afirmaram que 75% das organizações em todo o mundo sofreram algum tipo de ataque de phishing em 2020. Outros 35% sofreram ataques de spear phishing, e 65% enfrentaram ataques de comprometimento de e-mail corporativo (BEC.) De acordo com o FBI, Um BEC é "realizado por meio do comprometimento de contas de email comerciais legítimas por meio de engenharia social ou técnicas de invasão de computadores para realizar transferências não autorizadas de fundos". Em resumo, um BEC ocorre quando um funcionário recebe o que parece ser um email genuíno de um executivo superior. O email pede uma transferência de fundos para uma conta comercial falsa ou que forneçam informações pessoalmente identificáveis. O Internet Crime Complaint Center identifica cinco tipos de fraudes BEC: Fatura falsa, Fraude de CEO, Comprometimento de conta, Representação de advogado e Roubo de dados. De forma a minimizar a situação, as empresas estão a criar programas de educação e treino para ajudarem as suas equipas a reconhecer potenciais fraudes por email. As perdas decorrentes do comprometimento de e-mails comerciais (BEC) dispararam ao longo do último ano. O Relatório de Crimes na Internet do FBI mostra que em 2020, as fraudes em BEC fizeram mais de 1,8 mil milhões de dólares - mais do que através de qualquer outro tipo de crime cibernético.
Com o modelo P2T - Email Protector, aceitar uma notificação de um utilizador falso irá tornar impossível a libertação da mensagem retida porque o endereço fornecido não possui a mensagem desejada. Portanto, a divulgação de um endereço de email poderá ser incentivada e sem o medo de vir a ser usado por spammers.

- Botnets

Nos sistemas tradicionais, os utilizadores são infetados com algumas variantes de malware, permitindo a geração de bots automáticos e o envio involuntário de emails para as suas listas de endereços. Como esses bots não precisam pré-notificar os sistemas P2T, eles preenchem as listas de espera na OUTBOX, mas as mensagens nunca serão entregues, causando um alarme instantâneo na pasta Caixa de saída. Esse procedimento acaba tendo um papel preventivo e decisivo nos ataques de botnets.

- Emails em massa

Para estar a salvo dos efeitos do spam de email, os utilizadores tradicionais terão de investir tempo, recursos humanos e financeiros na ação de proteção. Agora, com o P2T - Email Protector, as ações de Email Directo, impõem uma responsabilidade acrescida no remetente para lidar com as mensagens indesejadas! Mas, por outro lado, os profissionais de marketing com o P2T - email Protector terão uma abrangente ferramenta de rastreamento e análise de campanhas que exibem eficaz e rapidamente os resultados. O P2T - Email Protector facilita recursos humanos, tecnológicos e financeiros para outras tarefas mais importantes.

Fazer mais com menos:

- Menor necessidade de recursos / Maior proteção concedida.

Algumas funcionalidades atualmente existentes, sugerem capacidades de operação adicionais de forma a convergirem para uma utilização mais rigorosa, no entanto isso não será mais necessário no modelo P2T. A simplicidade do seu uso traduz uma utilização mais justa e precisa. Estas são as de maior impacto.

Features	P2T	Google	Exchange	Yahoo	Apple Mail	Thundirbird
undosent	unlimited	30s	30s (owa)	✗	30s	✗
spamfolder	no need	✓	✓	✓	✓	✓
false positives/negatives	no need	✓	✓	✓	✓	✓
hardbounce	no need	✓	✓	✓	✓	✓
spam filtering	no need	✓	✓	✓	✓	✓
delivery/read confirmation	no need	✓	✓	✓	✓	✓
opt-in/opt-out	no need	✓	✓	✓	✓	✓
webmail	✓	Gmail	Outlook	✓	iCloud	✗
botnet threat (email)	✗	✓	✓	✓	✓	✓

6. Capacidade de Armazenamento

As organizações esforçam-se por otimizar o uso dos seus Centros de Dados e muitas vezes sentem-se forçadas a criar cotas para gerir as caixas de correio dos seus funcionários. Independentemente do destinatário decidir arquivar um email, deixá-lo para ler mais tarde, criar filtros para redirecionar para a pasta de spam ou até mesmo apagar, fazem todos parte de um conjunto de mensagens recebidas que foram depositadas livremente nos data centers pelos servidores de e-mail. E num dado momento, já tivemos como experiência o tédio de enviar uma mensagem para um destino e receber um erro de entrega "A caixa de correio do destinatário está cheia e não pode aceitar mais mensagens. Tente novamente mais tarde ou exclua mensagens para libertar mais espaço". Determinar o tamanho médio de uma mensagem de e-mail é difícil devido a vários fatores que entram em jogo. No entanto e em geral, um email médio é de cerca de 75KB de tamanho. Como 75KB tem cerca de 7.000 palavras em texto simples ou cerca de 37,5 páginas datilografadas, é facilmente percetível que outros fatores contribuem para o tamanho de um e-mail; I. as mensagens contêm informações de formatação para além do mero texto. II. Os emails de texto puro são frequentemente acompanhados por uma versão de texto simples duplicada da mesma mensagem. III. Newsletters e emails de marketing são geralmente emails maiores e neste caso constituem uma grande proporção de emails recebidos. IV. os anexos exponenciam fortemente a média. Embora alguns anexos sejam pequenos, alguns podem ter 10MB ou mais. V. photos, animações, clipes de áudio e outros anexos são adicionados ao tamanho. Os GIFs animados são particularmente famintos por espaço porque cada pixel é essencialmente uma imagem. Quanto mais pixels o GIF tiver, maior ele será. VI. o código HTML ocupa espaço. VII. num tópico de e-mail que vai e volta, o texto citado pode aparecer várias vezes. VIII. as informações de um cabeçalho que descrevem a rota do email não são visíveis, mas contam no tamanho. Os cabeçalhos têm um valor mínimo de cerca de 1KB e, em alguns casos, o valor máximo pode exceder devido a que cada router por onde esse email passa, adiciona mais informações.
Uma notificação P2T funciona como uma mensagem original, mas sem o corpo. O seu tamanho será equivalente ao de um cabeçalho. Em conclusão, pode-se dizer de maneira simplista que, 75 notificações P2T representam aproximadamente o tamanho de uma única mensagem.

7. Comparando ofertas

A tabela a seguir descreve as principais diferenças entre a oferta atual de mercado e a proposta de valor P2T:

Oferta de Mercado	Proposta de valor P2T
Capacidade de filtragem em 99,99%.	100% em capacidades de proteção.
Responsabilidade no destinatário.	Responsabilidade no remetente.
Propício a falsos-positivos/negativos.	Controlo de fluxo por seleção.
Permissivo a redes BotNet.	Incompatível com redes BotNet.
Facilitador de ocultação de Identidade.	Ação Não-repúdio.
Preocupação com a ocultação de endereços de email.	Partilha de endereços de email.
Largura de banda ocupada por mensagens não solicitadas.	Desempenho maximizado. Permissão apenas a tráfego autorizado.

8. Conclusão

"*Insanidade é fazer todos os dias a mesma coisa à espera de resultados diferentes*" O autor propôs uma mudança de paradigma a tudo o que nos últimos 50 anos foi oferecido como solução o que levou à proposta de alteração padrão de modelos de filtragem para Controlo de Fluxo por Seleção (FCbyS) oferecendo por consequência uma proteção mais justa para o destinatário. Seria essencial manter os atuais protocolos de comunicações de email optando apenas por alterar a forma como as mensagens seriam geridas dentro dos servidores P2T o que levou a criar novas regras internas para esse efeito. Desta forma tornou incompatível a qualquer utilizador abusador ou a redes botnet a ação direta e sem controlo de abusar do sistema. Todos os conteúdos de interesse serão a partir de agora responsabilidade do remetente fazer uma gestão de tudo aquilo que os destinatários não desejaram receber reforçando a necessidade de se manterem expostos na rede para as poderem libertar. A inversão desta responsabilidade é o pilar número um do sucesso deste projeto. Por fim, propôs a necessidade de reforçar a segurança e melhoramentos futuros com uma solução baseada em consenso por uma Organização Autónoma Descentralizada (DAO) mantendo a tendência e adaptação tecnológica de um futuro próximo.

9. Referências

[1] D. J. Bernstein, "Internet mail"
http://cr.yp.to/im2000.html

[2] Andrew Leung - TELUS Corporation, "SPAM – The Current State"
https://sicherheitskultur.at/pdfs/spam.pdf

[3] Tessian - Enterprise Email Security Software
https://www.tessian.com/blog/phishing-statistics-2020/

[4] Steve Morgan, Editor-in-Chief - Cybercrime Magazine
https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

[5] FBI - Internet Crime Complaint Center IC3
https://www.ic3.gov/Media/Y2019/PSA190910

Assinado por : **ANTÓNIO MANUEL DE JESUS PAIS**
Num. de Identificação: BI06266364
Data: 2021.05.11 10:07:13+01'00'

CHAVE MÓVEL