PROPRIEDADE INTELECTUAL E SEGURANÇA DA INFORMAÇÃO

Entrevista realizada pela Equipe Editorial da
Revista Tecnologias em Projeção

Ficha do entrevistado

Nome: Pedro Antônio Dourado de Rezende.

Curriculo: *Advanced to Candidacy for PhD* em Matemática Aplicada pela Universidade da Califórnia em Berkeley (1983), Bacharel (1975) e Mestre (1976) em Matemática pela Universidade de Brasília.

No vale do silício, trabalhou com controle de qualidade do sistema operacional Macintosh na Apple Computer, com sistemas de consulta a bases de dados por voz digitalizada na DataDial, e com as primeiras aplicações de hipertexto, precursoras da web, desenvolvendo *HyperCard stacks* para Macintoshes (1986 a 88).

Interesses profissionais incluem o estudo de métodos formais para análise e projeto de protocolos criptográficos; interesses pessoais, a linguística, a semiologia, a mitologia, a história e filosofia da ciência. A dissertação de doutorado, rejeitada em Berkeley, propõe um modelo algébrico para especificação de linguagens distributivas de máquina, e a pesquisa atual investiga o custo social dos modelos comerciais no setor da informática.

Professor concursado do Departamento de Ciência da Computação da Universidade de Brasília (UnB), onde tem lecionado, desde 1990, teoria da computação, teoria dos grafos, linguagens formais, linguagens de programação, compiladores, organização de hardware e software, criptografia e segurança de dados, informática e sociedade, entre outras disciplinas, e exercido os cargos de coordenador do Bacharelado em Ciência da Computação, do Laboratório de Informática, e do ensino básico de programação. Foi também professor no Departamento de Matemática da UnB (1976 a 78) e na National Hispanic University (EUA, 1986).

Participações no Grupo de Padronização de Segurança da Comissão de Informatização do Conselho Nacional de Justiça (2006), no Grupo Interministerial sobre Sociedade da Informação no Itamaraty (2005), no Conselho do Instituto Brasileiro de Política e Direito de Informática, no Conselho da Free Software Foundation Latin America (2007 a 2008), e no Comitê Gestor da Infra-estrutura de Chaves Públicas Brasileira, ICP-Brasil (2003 a 2006), como representante da Sociedade Civil por designação do Presidente da República.

Consultor em criptografia e segurança

computacional para empresas, órgãos públicos, legisladores, operadores do Direito e agências de fomento científico no Brasil, Assessor especial da Presidência do Instituto Nacional de Tecnologia da Informação para assuntos internacionais relativos a propriedade imaterial e software livre (2005), Coordenador e professor, desde 1997, do Programa de Extensão em Criptografia e Segurança Computacional na UnB, o primeiro a oferecer no Brasil (2003) curso de programação para Infraestruturas de Chaves Públicas.

Autor de mais de uma centena de artigos e ensaios sobre criptografia, segurança na informática, evolução dos vírus digitais e programas maliciosos, sobre software livre, revolução digital, paradigmas computacionais e epistemologia da ciência. Palestrante em congressos, seminários e audiências públicas sobre segurança na informática, sua relação com o Direito e a cidadania, no Brasil e no exterior. Co-autor do livro "Burla Eletrônica", sobre vulnerabilidades do sistema eleitoral informatizado em uso no Brasil, e da coluna "Segurança, Bits & Cia." (2002 a 2003), no Jornal do Comércio do Rio de Janeiro.

Dentre as atividades acadêmicas tem orientado projetos de graduação pioneiros na área de criptografia e segurança computacional, tais como o primeiro *firewall* TCP/IP no Brasil (1995), a primeira biblioteca auditável com criptografia robusta para ICPs no Brasil (1998), um sistema de editoração personalizada com identificação de cópia por marca d'água digital (1999), um protocolo para monitoramento da custódia de chaves privadas (2003), e o primeiro protótipo de *middleware* para controle de processos judiciais eletrônicos baseado em papéis (RBAC) e certificados x.509 (2006), com alunos que têm se destacado com prêmios.

Dentre alunos premiados, Luiz Rios e Karlei Rodrigues, com o prêmio e-COBRA pelo melhor plano de negócio em comércio eletrônico no Brasil (sistema de editoração personalizada, CopyMarket, 2000); Alexandre Gomes, com o SOUJAVA Motorola/Nextel/Sun (software para centrais de pagamentos via telefonia móvel, Foton, 2001) e com o J2ME/Nokia (Mobile Financial Manager, SEA, 2003); e Daniel Ramagem, com o 3o. prêmio SSAI International Semantic Web Challenge ('AnnoTerra', Science Systems, 2003).

Entrevistador: Qual o trabalho mais relevante da sua carreira

Dr. Pedro A.D. Rezende: Posso listar algumas. Minha participação como ativista em políticas públicas de informática, de TI, no início do governo Lula como ativista. Também o trabalho que eu faço na interface com direito, também como ativista. Sou conselheiro do instituto brasileiro de política de direito de informática. Algumas orientações de projetos finais que foram premiadas, como por exemplo, o melhor plano de negócio na internet no ano de 2000 e alguns outros trabalhos pioneiros.

Entrevistador: Dr. Pedro, fale um pouco sobre propriedade intelectual:

Dr. Pedro A.D. Rezende: Eu acho que propriedade intelectual é um conceito perigoso por que esta sendo abusado no mundo inteiro, nesse estágio do capitalismo para encastelar as imposições e, economias que já passaram pela faze de industrialização como economias rentistas que vão viver de cobrar pedágio do resto do mundo. Eu acho que é uma proposta perdedora para o Brasil apostar nisso.

O Brasil deveria ter consciência de que isso é um jogo de cartas marcadas. O Brasil só tem a perder aceitando esse jogo, é como se tivéssemos que competir com o casco de tartaruga numa corrida contra Aquiles.

O jogo de propriedade intelectual só serve aos interesses concentradores de legitimação consentida de capitais para a sobrevida dos modelos de negócio que estão já obsoletos, para o estágio do capitalismo que nós estamos vivendo hoje. Nós vamos entrar num período de escassez de recursos naturais que vai criar muita tensão geopolítica no planeta e essa história da propriedade intelectual funciona como uma legitimação consentida de um novo regime de escravidão através do controle do conhecimento e da circulação da informação.

É isso que eu penso sobre a propriedade da informação. Por isso meu ativismo contra a radicalização, contra o que a gente esta vivendo hoje no regime de patentes de software e em inúmeros debates e palestras que eu já concedi, (estão todas no meu portal)

Entrevistador: Já existem alguns países que estejam seguindo esse modelo que o senhor prega?

Dr. Pedro A.D. Rezende: Esse meu pensamento de que regimes de propriedade intelectual muito radicais e rígidos, que querem regular tudo, não dão certo. São um tiro pela culatra. Isso aconteceu na Europa no final do século 19. Alguns países abandonaram completamente o regime de patentes se não me

enganou: Bélgica, na virada do sec. 19 pro sec. 20. Depois voltaram. Isso eu acho que é a dinâmica natural do capitalismo. O capitalismo sobrevive da ampliação do mercado, então a propriedade intelectual é a forma encontrada para se continuar expandindo mercado, agora, através do controle da circulação e do uso do conhecimento útil que pode gerar eficiência econômica.

Propriedade intelectual em si é uma contradição em termos. Propriedade é algo que restringe, e intelecto só existe quando é compartilhado, então, é um termo contraditório dependendo do lado que você puxa. Se ele for radicalizado, vira um regime jurídico que da força excessiva a quem tem o poder econômico de controlar a circulação da informação que hoje é o que beneficia quem quer acumular capital.

Entrevistador: Nos ataques as páginas do governo é possível que tenha havido roubo de informações?

Dr. Pedro A.D. Rezende: É possível. A credito também que se ocorreu mesmo, não seria admitido a menos que por necessidade, a menos que venha a publico, por exemplo, lista de senha escancaradas, e isso é normal, é compreensível, nessa área ninguém gosta de admitir. Você já viu algum banco admitindo que sofreram invasão ou fraude? No entanto, você sabe agora pela boca da policia federal que boa parte do trabalho deles é correr atrás de quem aplica golpes eletrônicos. A briga ai é política, ideológica pra ver quem fica com a conta de correr atrás do prejuízo.

No caso de pirataria, que é o acesso ilegal a obra autoral e fraude bancária, o que os grandes interesses, os grandes empreendimentos nessas áreas gostariam, e estão tentando é convencer a sociedade de que isso é uma luta não deles, que ficam com o privilégio da eficiência econômica trazido pela tecnologia, mas da sociedade, por que eles querem que isso seja tratado como um problema social, a migração da atividade criminosa para o espaço cibernético, para uso da tecnologia como um instrumento e não como uma contrapartida da facilidade. Eu vejo a facilidade do crime criminoso que usa TI ficar impune, ou contrapartida, da facilidade de que as pessoas tem de ganhar dinheiro e de se comunicar usando a internet. É o outro lado a mesma moeda.

Entrevistador: O governo brasileiro tem uma política de segurança realmente confiável?

Dr. Pedro A.D. Rezende: Olha, política de segurança é uma coisa que deveria ser não só de governo, mas de qualquer entidade. Quando você pergunta se do governo é confiável para ele, eu acho que é. Agora não é uma política de

segurança, digamos homogênea, coesa, empregada e fiscalizada por igual em todos os órgãos, e é natural que seja assim, por que cada órgão tem seu perfil.

Cada órgão tem sua missão e por causa da sua missão tem o seu perfil de riscos de interesses que podem ser contrariados, e sua competência pra gerir sua própria infra-estrutura, seu legado histórico de como foi feito o investimento nessa área, através das diversas administrações.

Não é uma tarefa fácil implementar uma política única de segurança na informática de um governo. Quando a gente tem 3 estâncias de governo, federal, estadual e municipal, a gente tem 3 poderes no governo republicano democrático como e o nosso, executivo, legislativo e judiciário. Pra ficar só no executivo, onde ainda ha um esforço de padronização, com a iniciativa inicialmente da casa militar e depois da casa civil e depois da casa militar e agora passou pra casa da defesa, de ordenar uma política comum de segurança da informática.

Agora, mesmo que tivesse uma política de segurança homogênea que é mais fácil de dar certo num governo autoritário, um governo não democrático, do que num que ainda esta amadurecendo na sua formação democrática, como é o nosso, ainda que tivesse uma, eu não acredito que não seria eficaz em relação ao que esta em jogo na geopolítica hoje, o Brasil é um país que senta em cima de recursos naturais que vão ficar escassos em algum momento, que ninguém se iluda que isso atrai a cobiça de interesses que não vêem na soberania de um estado nação como o Brasil uma barreira ou empecilho pra se apropriar desses recursos quando julgarem necessário ou conveniente, ou seja, o Pré-sal, seja água doce, seja terra agriculturável, terra arável.

O Brasil detém 98% das reservas de nióbio do planeta, no entanto não existe uma política de controle e precificação desse mineral estratégico que é usado pra metalurgia de alta performance, em foguetes, em armamento de guerra, aviões de caça, então o Brasil não tem nenhuma política industrial pra defender e preservar seus recursos da altura do tamanho do desafio, quanto mais uma política de segurança da informática. e se tivesse uma eu acredito que ela não seria eficaz por que o estado que estamos hoje na informática é praticamente indefensável, a gente vive numa monocultura de software, software de uma complexidade próximo do não administrável, a quantidade de vulnerabilidades que são descobertas todo dia e a forma como o crime organizado já esta evoluído ao ponto de saber como tirar proveito disso e como vender o uso dos seus conhecimentos pra quem pagar melhor, inclusive sem deixar rastros,

isso a gente esta vendo todo dia nas listas de descrição de segurança, não vai ter política de segurança que contenha o quadro atual da guerra cibernética que a gente esta vivendo. é uma guerra pra valer! é como se a guerra fria estivesse migrando pro espaço cibernético.

Ou seja, não estou justificando que uma política de segurança pouco adequada, ou pouco amadurecida, ou com pouca força política pra ser implementada. O que eu estou dizendo não é pra justificar uma situação dessas, caso essa seja a situação do Brasil atual. O que estou dizendo é que não vale apostar nisso com uma solução pra situação que a gente esta vivendo.

Uma política mais eficiente de informática hoje apenas daria mais trabalho a quem tem mais interesse em só falar a eficácia do estado em cumprir sua função no nosso país, administrar os recursos se mostrar eficiente. E esse jogo pode ser usado pra justificar decisões que implicam em perda de soberania em relação à legislação.

Esse negócio de combater o crime digital no planeta inteiro e por conta disso combater o crime digital que esta no planeta inteiro, passar o poder para outros organismos transnacionais, de prender, de sequestrar de bloquear fluxos ou bens simbólicos, é uma jogada ingênua e arriscada, então tem que tomar cuidado com essa historia de que a gente foi pego de surpresa nessa guerra cibernética, que estamos despreparados, que temos que fazer alguma coisa, certas coisas que podem ser feitas podem ser pior do que o que a gente já tem, na minha opinião.

Entrevistador: Quais áreas da segurança da informação estão com maior deficiência de profissionais?

Pedro A.D. Rezende: Praticamente todas por que a área de segurança na informática, ela requer um conhecimento em todas as outras áreas da informática, em engenharia de software, em criptografia,, conhecimento também dos processos administrativos, de engenharia de redes, e esse conhecimento não se adquire sem um processo de formação que tem o seu tempo, então não é só em segurança informática que o Brasil tem deficiência.

O Brasil tem deficiência técnica na área de informática como um todo e em várias outras áreas. O professor Sílvio Meira, que já foi presidente do SBC, e gosta também de escrever sobre o aspecto social da computação, e ele tem recentemente falado bastante que o Brasil tem uma deficiência grande em engenharia de software. Ele vê a engenharia de software como um caminho pra resolver essas difíceis todas. Eu

tendo a concordar com ele, mas não como a solução mágica, em relação à segurança na informática, falta tanto conhecimento técnico como conhecimento geral, cultural e político, o que enfim, no final das contas, no frigor dos ovos a informática é um instrumento de poder hoje, e se você não perceber como a informática é um instrumento de poder, você que tem competência técnica, pode se ver de repente envolvido em situações onde você vai estar numa guerra dando tiro pro lado onde sua consciência acha que é errado. Se você não tiver essa percepção, você pode ser envolvido. a segurança é ao mesmo tempo um processo que envolve probabilidade, riscos, incidentes.

O risco envolve a probabilidade de incidentes e os valores que podem ser perdidos nesses incidentes. Então medidas que buscam controlar as probabilidades ou a dificuldade de incidentes serem praticados com intenção de causar dano, é uma parte do processo. O contexto onde essas medidas podem ser eficaz é 90% do processo, e identificar como e de que maneira escolher as medidas e mecanismos de proteção para que possam ser eficazes, é a parte do processo de segurança que acontece na fronteira do processo político, então se o técnico não tiver consciência destas coisas pode, por exemplo muitos dos criminosos nos EUA hoje estão - tem o artigo do *Guardian*, jornal inglês, coisa de umas 3 semanas atrás - dizendo que a metade dos hackers - hackers no sentido pejorativo que vem sendo usado pela mídia pra se referir aqueles que usam informática para agir de formas ilícitas ou condenáveis - aqueles que são pegos pela policia federal americana, FBI, eles estão sendo cooptados, os americanos aprenderam isso com os chineses, eles são convidados sobre mando da policia federal, para não serem processados e não irem pra cadeia, ele tem a opção de passar a trabalhar sobre as ordens da policia federal, com ou sem pagamento dependendo da dificuldade da tarefa ou então o processo andar, se o próprio processo não andar pra eles não serem processados e condenados, são oferecidos alternativas de trabalhar para o FBI em conversa, eles continuam agindo como se fossem bandidos independentes, mas cumprindo ordens da policia. alguns até são contratados por grandes empresas também.

Também mas isso não por que são pegos e são colocados contra a parede pelas empresas, geralmente é por que eles preferem correr menos riscos e preferem trabalhar ao abrigo de um negócio legado. muito que começam nessa zona cinzenta de estar vendendo serviços pra qualquer um e acabam trabalhando com exclusividade para uma empresa que do ponto de vista de como ela esta agindo no mercado, ela pode está agindo sem ética em

outro plano mas no plano trabalhista não. Quem esta trabalhando ali pra...

O Stuxnet, por exemplo, quem fez? Isso e uma arma de código, uma arma que é hoje esta sendo adaptado pra atacar qualquer processo de controle industrial que se queira refinaria, oleoduto, companhia elétrico, esta dentro, ai nos sites das quadrilhas. Quem fez essa arma e soltou pra derrubar as centrifugas no Irã, pesou nisso? Nessas consequências? Se pensou e o não, teve uma reação quando viu que ela estava sendo adaptada para situações que poderia fazer dano a ele mesmo. Eu vejo assim a declaração do governo americano de que guerra cibernética agora é escancarada, declarada, quem fizer coisas parecidas como que os Stuxnet fez no Irã e nos EUA, mesmo que a identificação da origem não seja positiva ela vai ser alvo de retaliação militar.

Então dependendo de onde você olha, trabalhar numa empresa que atua na área de segurança é ética no plano de relações trabalhistas, mas pode não ser dependendo do serviço que a empresa esta prestando ao cliente. Qual é o serviço? Qual o objetivo do que ela ta fazendo? Se é fazer antivírus pra quem quer defender o sistema que não tem concerto, que não vai poder ser melhorado, que não da autonomia decidir o que vai acontecer dentro ad sua maquina, pra mim é tão antiético quanto tentar mudar essa situação. eu quis dizer diferente, é menos ético do que tentar agir de uma forma que mude esse estagio hoje. Por que a gente é tão dependente da informática hoje?

Entrevistador: Você acha que a área da segurança exerce um papel de importância que deveria ter nas empresas?

Pedro A.D. Rezende: Acho que não tanto. Acho que as empresas são mais imediatistas em relação ao balancete, o investimento que não gera retorno imediato sai do radar de quem toma a decisão, e tem muita empresa que não da a devida importância a área de segurança na sua estrutura de TI, infelizmente. Mas isso é próprio dos tempos que a gente esta vivendo, eu acho que a ciberguerra vai alterar um pouco essa visão. A legislação esta sendo eficaz? A que virá é pior do que a que tem. O problema não é com a legislação. A dificuldade em relação ao que esta acontecendo hoje, não é a falta de lei, é ninguém ter levado em conta que as maravilhas da tecnologia têm... Em um mundo onde as pessoas estão dando pouca importância a ética, a TI vai ser explorada pelo crime sim. Não vai ser lei que vai resolver. o que as leis sendo propostas no mundo inteiro estão tentando fazer? Estão tentando aumentar as penas, diminuir o rigor do que é prova diminuir as garantias dos

processos e em alguns casos eliminando o devido processo legal, dando o poder de punir a polícia a dom de interesse que é supostamente contrariado. Então a gente tá voltando ao tempo em que o direito não tinha as garantias que a revolução francesa e o ressurgimento que a democracia trouxeram. Nem esta também solapando as garantias que o direito romano trouxe. Por que os países gostavam de entrar no plano romano? Não se importavam de ser conquistados? Por que eles viam que tinha mais a ganhar com a estabilidade que participar do sistema jurídico romano trazia pra eles. Era uma forma de administrar a justiça que era mais eficiente do que muito tinham.

Então muitos países por vontade própria eram conquistados e não se rebelavam contra as conquistas, por que convinha a eles ser pacificados pelo sistema jurídico romano. Então toda a tradição do direito romano de dar garantias, direito de quem está sendo acusado de ser ouvido, tudo isso está sendo esmagado com essas reformas jurídicas: tratados de cibercrime, tratado ACTA, lei do AI 5 digital que é a lei de crimes cibernéticos que está transitando no congresso, essas leis vão dar mais poder a polícia de, vai coagir provedores de acesso a operarem como polícia, a agirem como espões sobre penas de serem eles punidos se não agirem assim, vai dar poder a polícia não só de espionar mas também de agir na posição de juízes, no caso do Three Strike Rule de tirar as pessoas da internet por mera acusação de pirataria repetida, as pessoas podem se ver punidas com a revogação de um direito sem que tenha havido um processo de julgamento onde ela possa se defender, e numa situação onde 10% das máquinas são controladas por Botnet, isso é um risco muito grande por que é plausível que alguns tenham sua máquina usada pra cometer crimes da mesma maneira que é plausível que quem cometeu o crime alegue que sua máquina tava dominada por uma quadrilha como uma forma de defesa.

Então não vão ser leis mais severas que dão mais poder ao estado pra julgar sem as devidas garantias pra quem é acusado, que vai resolver o problema. Vai tornar o estado mais poderoso, a sociedade mais dependente do estado, numa situação em que o estado está falindo na sua missão de proteger os direitos dos cidadãos também, e não só os proteger os interesses econômicos que estão se vendo ameaçados com o crime migrando para a internet. O crime sempre existiu, e a falta de ética na sociedade como um todo está se refletindo de todos os lados, a democracia está sendo corroída por dentro com essa solução "mágica" de leis mais severas, ou o crime organizado, tendo uma forma mais eficiente de agir longe do braço do

estado por que é mais difícil identificar a autoria, e o cidadão pego no meio desse cabo-de-guerra.

O que vocês precisam entender é o seguinte, o papel do estado está mudando com a revolução digital e pra ele está cada vez mais claro que a única forma de sobreviver é se aliar aos interesses do capital. e onde fica o cidadão nisso? Onde ficam as conquistas da tradição do direito comum e da revolução francesa que fez ressurgir a democracia? Enquanto não estiver faltando comida no mundo provavelmente as pessoas vão achar que essa troca vale a pena, elas vão se sentir mais protegidas. Mas quando o estado virar o vilão? Quando o estado achar que precisa cometer limpeza étnica pra sobreviver como estado, como aconteceu na Iugoslávia, pode acontecer na Síria, como está perigoso acontecer em algumas regiões do Oriente Médio. O estado com mais poder legitimado por um parlamento que preteja combater o crime cibernético tá dentro do processo democrático dentro do estado, isso vai ser bom ou vai ser ruim?

A História nós conta histórias parecidas, é melhor a gente prestar atenção na história. Qualquer solução imediatista de leis mais severas, de investimento nessa ou naquela tecnologia ou nessa linha de formação não é solução, pode ser até pior, por que o problema é no sistema. A informática está capitalizando, tornando mais ágil as transformações que esse estado de coisas proporciona, por que a informática é um instrumento de poder cada vez maior, quem controla o fluxo de informações hoje controla preço, quem controla preço tem vantagem comercial, isso tudo é.

Entrevistador: Nos fale sobre o reflexo da Cloud Computing sobre a área de segurança:

Pedro A.D. Rezende: Bem, eu acho que esta história está mal contada. O problema da Cloud Computing é a solução pra menor custo em gerir TI hoje. Fica mais vulnerável no sentido de que você perde o controle direto sobre os seus dados. Amanhã se você quiser acessar os seus dados ninguém lhe garante que você vai poder. Não vai ser a letra de um contrato que vai fazer o *Data Center* funcionar se amanhã o *Data Center* onde estão os seus dados, ou a fazenda, a rede de *Data Center* onde estão seus dados for interditado ou sequestrado pelo governo nacional. Uma das coisas que quem vende serviços de Cloud Computing faz que é uma esperteza de negócio é dizer que não pode divulgar onde estão suas máquinas, justamente pra não atrair criminosos, que vão querer atacá-las ao estilo de piratas, pra poder extorquir dinheiro em troca de deixar em paz, que é o que faz a máfia. Tudo bem, mas se você quiser fazer valer o seu

contrato amanhã caso o serviço seja interrompido por que você não tem mais acesso aos dados, o que vai adiantar o contrato? Se você não tem onde mandar o oficial de justiça capturar o HD pra você ler seus dados.

Nada é fácil nessa área de segurança, tudo tem outro lado. Então do ponto de vista do custo, o Cloud Computing é uma solução atraente e que sai mais barato. Manter um serviço onde você só precisa manter uma rede que usa navegador pra acessar os dados ao invés de manter uma infraestrutura...

Entrevista: Qual a importância do software na área de segurança digital?

Pedro A.D. Rezende: Isso é um assunto de um artigo que estou para escrever a algum tempo, do ponto de vista das vulnerabilidades, a vantagem mais importante que eu vejo no software livre, o fato de não a como quem faz o software esconder porta de fundo (backdoor) no software de outros desenvolvedores que tem interesse no mesmo código.

Embora vulnerabilidades possam ser exploradas para penetrar sistemas, as portas de fundo que são colocadas no software que só é distribuído em formato digital, formato executável, que não pode ser compilado no ambiente onde será executado, tem um diferencial, eu acredito, em relação as outras vulnerabilidades as outras maneiras de penetrar sistemas que decorrem das vulnerabilidades que existem tanto em software livre como em software proprietário.

Primeiro uma porta de fundo que é oculta no software que é distribuído só em binário, como no software proprietário, que a gente já deve passar por cima da fase de ingenuidade de alguém está perguntando se existem ou não existem, existem portas de fundo documentadas que foram descobertas por acaso, no sistema operacional Windows por exemplo, uma delas 15 anos depois de que foi introduzida.

É por que que elas não são a mesma coisa do que uma porta de fundo que é construída em cima de uma vulnerabilidade em código que está disponível para qualquer um ver e auditar? Primeiro porque uma porta de fundo que é escondida em código proprietário, que não é distribuído com o fonte, você não tem como chegar a ela pela funcionalidade do software, e não será estudando o software que descoberto, você vai descobrir ela por algum acaso, ela não vai aparecer como em um estudo de vulnerabilidade em cima do binário, então quem colocou ela lá na hora de compilar e escondeu ela dentro do binário na compilação, como é código que não tem acionamento pela funcionalidade disponível pelo usuário, não tem como aquilo

aparecer no estudo de vulnerabilidade do software executado, vai ficar escondido e ninguém vai descobrir se não for por acaso.

As portas de fundo que existem em software livre são só do tipo via vulnerabilidade, elas não estão ali escondidas por quem fez o software, as portas de fundo em software livre elas surgem da exploração de vulnerabilidades que não são concertadas a tempo, quem tá usando sofre.

Então isso dá um tipo de vida útil e uma chance de conhecer a porta de fundo diferenciada para quem faz o software proprietário, para quem usa, e para quem faz e usa software livre, quem faz software proprietário tem muito mais poder de explorar vulnerabilidade de forma oculta, por exemplo vendendo para o governo, para CIA ou FBI por exemplo, e muito mais poder de vender acesso oculto aos usuários do quem que está no crime organizado para vender o mesmo serviço, esses só vão ter acessos as portas de fundo que são abertas, pela exploração de vulnerabilidade que podem ser descobertas, agora as vulnerabilidades que podem ser descobertas no software livre são todas e as que podem ser descobertas no software proprietário são parte, tem aquelas que são ocultas inclusive na funcionalidade do software.

Entrevistador: Até hoje pode haver algumas escondidas?

Pedro A.D. Rezende: Até hoje podem ter sim, se teve uma porta de fundo para executar código executável como administrador, em código escondido como comentário em formato de imagem, no formato wmf, ficou escondido esse recurso durante 15 anos a pretexto de que aquilo era necessário para mandar mensagens de erro da impressora para o sistema. Podem ter outras como tinha uma chave da NSA de autenticação de código de biblioteca criptografia no windows descoberto em 2000 com uma busca binária em cima do executável isto aí foi uma garimpagem descoberta por acaso, então nesse estágio que a gente está vivendo, eu acho que qualquer governo que quer ter soberania que queria defender a sua, ele tem que considerar isso, eu não estou entrando na discussão se o fato de que código está disponível para todos verem ajuda ou não a encontrar as vulnerabilidades e a corrigir a tempo, se ajuda ou não quem quiser corrigir por conta própria, corrigir a sua, independente do fornecedor que quer ou não quer atualizar o binário para corrigir.

Entrevistador: Atualmente qual é o maior obstáculo para as consultorias que atuam na área de segurança digital?

Pedro A.D. Rezende: Confiança

Entrevistador: Confiança?

Pedro A.D. Rezende: A mercadoria na área de segurança e confiança, como e que você irá mostrar suas credenciais para o seu cliente, como é que você vai levar o seu cliente a acreditar que você tem competência para deixá-lo em uma situação melhor em relação às vulnerabilidades que ele está exposto.

Por que é muito fácil fazer o teatro passar por processo, eu vivo dizendo que segurança e teatro e processo, o que que é sentimento e processo, o que é processo? É probabilidade de ocorrer um incidente, danos, quando os incidentes e fortuito, acontece por acaso, segurança tem um nome específico em inglês que é *safed*, em português nos só temos uma palavra para falar de segurança: segurança, em inglês a palavra para incidente que envolve a intenção maliciosa de alguém para causar dano e chamada de security, diferente de *safed*, security seria o processo para controlar a proteção contra intenção maliciosa, e *safed* o processo para proteção contra incidentes fortuitos como: caiu um raio, pegar fogo no prédio, no-break, essas coisas.

Então falando de security, na segurança contra a má-fé de alguém que pode se aproveitar da fragilidade da comunicação como ela e hoje intermediada em T.I. Para enganar alguém, o processo e você mapear aonde estão os riscos, o que você poderá perder, onde você pode ser enganado e tentar agir para controlar essas probabilidades e esses riscos, com alguns mecanismos que te diminuirão essas chances, mas também com administração e gestão adequada do processo, e o outro lado da segurança e pessoal e o sentimento, e você acha que o risco que esta exposto e inevitável ou tolerável ou não. Então não tem como você mapear o sentimento para processo do mesmo jeito que todo mundo, tem gente que vai entender o que é uma situação de risco no uso de T.I. De um jeito que o faz sentir desprotegido ou incomodado ou em uma situação inaceitável, outro vai achar que se a empresa tá ganhando dinheiro agora desse jeito e melhor não desviar dinheiro para tentar interferir naquele risco por que o risco ainda não se materializou para ele então não existe, não tem como você evitar completamente os riscos sempre tem alguém que você tem que vai está exposto ao risco.

Então segurança em relação ao plano do sentimento (do ponto de vista pessoal) e uma situação de risco aceitável, e segurança como processo e você atuar nos processos de comunicação para controlar os riscos é evitar perdas e danos a um nível aceitável, mas o que é aceitável? Pode ou não ter haver como você

entender os processos e as probabilidades se tem haver com você entendendo probabilidades e processo você tá usando um critério de política de segurança para dizer até onde você vai na tentativa de controlar os riscos até onde você vai deixar para o acaso que não compensa você investir, seria paranoia, se você usa o sentimento para julgar os limites do processo de segurança onde convém você intervir isso e política de segurança, mas se você vai tomar decisões com base apenas nos sentimentos sem entender os processos, isso é chamado de teatro, entendeu? Muita empresa atua na área de segurança puramente no plano teatro, toma decisões a respeito de segurança com base apenas na intuição sem entender os processos, o executivo quando tem que tomar as decisões ele vai apenas de orelha tá entendendo de onde está vindo essas probabilidades de risco, e quem está informando o executivo para ele tomar essa decisão, também pode está traduzindo para ele riscos da maneira que convém a ele intermediário, a ele puxar mais poder, intuitivamente todos sabem disso, então uma empresa que vai presta consultoria de segurança ela precisará saber atuar no teatro porque em quem confiar para tomar as decisões ou fazer as coisas é o primeiro passo importante para política, se você não tem uma carteira de clientes para começar, você está com o problema de ovo da galinha, como e que você vai começar? Entende? Se você for competente alguém pode agir no teatro para induzir no seu potencial cliente a duvida de sua competência ou duvidar de suas intenções, tomando o seu cliente, e você pode achar que o jeito de ganhar dinheiro, já que não está conseguindo sendo honesto e enganar o cliente a respeito do que você é capaz de fazer e de garantir, então contrato e papel na área de segurança não vale muita coisa, o que vale e confiança, confiança é um dos assuntos mais difícil de se lidar do ponto de vista científico.

Entrevistador: É o uso de redes sociais como ela afeta a segurança das pessoas?

Pedro A.D. Rezende: Pois é ai e que tá, na rede social você requer equiparar as interações que você tem com as pessoas que o fazem o ser social no mundo que existia antes da internet, mas as pessoas costumam a perceber que existe uma grande diferença nas duas formas de criar uma vida social, no mundo sem os bits a internet e os computadores a maneira de você ter uma vida social e interagindo com as pessoas no seu meio físico, entrando em contato com as pessoas, com esse contato físico existe uma gama enorme no processo de comunicação que acontecem que fazem as pessoas criar imagens umas das outras no qual estão baseados as

relações de confiança que criam as identidades de amizades, de uma querer seguir o outro e etc, quando você quer transporta esse processo para o mundo dos bits você tá querendo arremedar o que acontece no mundo da vida, de carne e osso, mas sem os mesmo laços, ai oque acontece, as pessoas percebem que podem mentir mais facilmente sem serem descobertas nisso, ai fica num mundo de fantasia e de me engana que eu gosto, e ai fica a imagem que as pessoas tendem a concentrar sua vida social naquilo que tá sendo praticado através dos bits que então levam elas a afrouxarem ainda mais os seus critérios éticos de como elas se devem conduzir na vida, e eu vejo esse efeito, por um lado e benéfico pois você dá a oportunidade a todos de terem uma vida social livre, porém é uma tentação para as pessoas afrouxarem seus critérios morais e éticos ao viverem em sociedade e se já é um problema da sociedade a situação que a gente está vivendo de pouca gente e pouca importância dada aos valores morais, então nesse sentido a como eu disse a informática entra para agilizar o processo de degradação.

Entrevistador: Concluindo e fazendo uma previsão também, quando você acha que isso vai interagir para dar certo?

Pedro A.D. Rezende: Da certo eu não sei, mas o desfecho disso está previsto no livro de Apocalipse.

Entrevistador: Qual é esse desfecho?

Pedro A.D. Rezende: É um governo global, totalitário, que vai controlar tudo que as pessoas podem e não podem fazer, inclusive a liberdade religiosa, até lá a igreja de cristo já não deve mais está aqui se a doutrina do arrebatamento, pré tribulação estiver acontecendo.