Número 012 - Ano I - 01 de setembro de 2003

CFSEC security architects

-do-not-cross-

Manchete

Vírus de computador ganham destaque na grande mídia

*O vírus Lovsan, que ataca os computadores que funcionam com o sistema operacional Windows, causou grandes estragos hoje na Ásia: milhares de máquinas começaram a acender e apagar, à revelia do comando de seus usuários. (**Folha de São Paulo**)*

*Os engenheiros da Japan Post devem determinar quantos computadores foram atingidos e a suspensão de comunicações internas durará dois ou três dias, segundo as mesmas fontes. A companhia pública informou que seus serviços de contabilidade e finanças não serão afetados pela interrupção. (**Jornal do Brasil**)*

*Fabricantes de antivírus detectaram o retorno do vírus Sobig, que apareceu pela primeira vez em junho último. O MsBlast reaparece também, agora travestido de mocinho. (**O Estado de São Paulo**)*

*Just as these problems seemed to be receding, the latest version of a virus called SoBig invaded many computers in the form of attachments to e-mail notes. When an unwary user opened such an attachment, the virus could steal all the e-mail addresses residing on the computer and mail copies of itself to those people as well, Inviting the unwary to click on the attachment and start the infection moving again. (**The New York Times**)*

Ponto de vista da CFSEC:

O cafezinho ainda é mais importante do que segurança da informação!

No ***–do-not-cross-*** de 18 de novembro de 2002 (dnc20021118.pdf), comentávamos sobre o artigo escrito por ***Tom Standage*** para a revista ***The Economist***, cujo título era ***Securing the cloud***. Nesse artigo, Standage mostra numa matemática simples, que as empresas gastam mais com cafezinho do que com segurança.

Depois desse último mês, podemos chegar a conclusão que tal qual o momento do cafezinho, impera a descontração e certa ausência de seriedade no tratamento de pragas de computador pela maioria das grandes, médias e pequenas organizações pelo mundo (incluindo Brasil).

Toda semana surgem diversos tipos de vírus e suas variantes eletrônicas (worms, trojans, etc.), mas nas últimas semanas, imperou a perplexidade de vermos algumas dessas pragas, virarem manchete fora das páginas especializadas em informática.

O mais fantástico é que não é preciso que se inventem novas maneiras de levar o mundo informatizado à polvorosa. Basta explorar uma vulnerabilidade publicada do sistema operacional mais utilizado (Microsoft Windows), já que, certamente, uma quantidade imensa de organizações não fazem as correções sugeridas pelo fabricante.

Continua...

Ponto de vista da CFSEC: *continuação*.

Anos atrás, os atacantes aguardavam meses para que uma vulnerabilidade importante fosse esquecida para usarem formas de explorar os ambientes vulneráveis. No mês passado, nós publicamos aqui no ***–do-not-cross-*** como o resto do mundo publicou, a grande vulnerabilidade nos sistemas Microsoft Windows. Duas semanas depois, um vírus eletrônico se aproveita dos ambientes onde a falha ainda não havia sido corrigida e se propaga de forma assustadora.

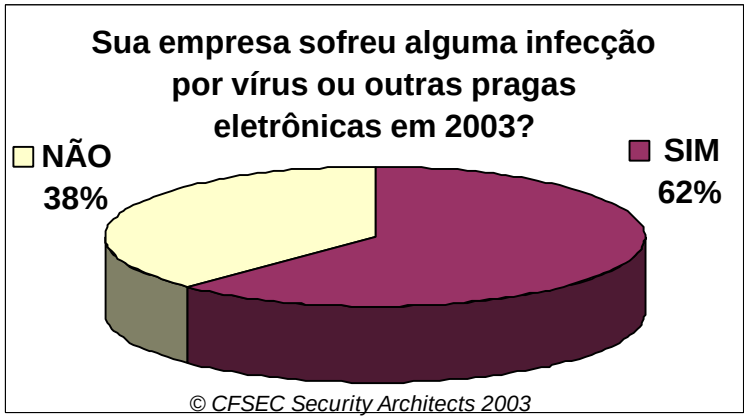
Como que ainda embriagados por esta contaminação, um novo vírus se espalhou também com muita velocidade causando grande prejuízo às organizações do mundo todo. Sua forma de contaminação? Arquivo executável anexado ao e-mail!

Falta seriedade para manter os ambientes atualizados. Falta coragem para encarar a divulgação e campanhas de conscientização da política de segurança. E, falta principalmente, levar a Segurança da Informação para um nível mais alto de gerenciamento. Bem, pelo menos alguns amigos têm aumentado seu capital investindo na NASDAQ, em ações de desenvolvedores de antivírus.

PESQUISA DO MÊS:

Como você se relaciona com pragas eletrônicas?

Neste mês, a pesquisa do site www.cfsec.com.br foi sobre como as empresas têm lidado com vírus e outras pragas eletrônicas. Na verdade, não nos surpreendemos com os resultados, pois muito dificilmente estaríamos numa situação diferente da que é encontrada em pesquisas por todo o mundo. Se você tem problemas com vírus e quer ouvir nossa opinião, informe-se por info@cfsec.com.br.

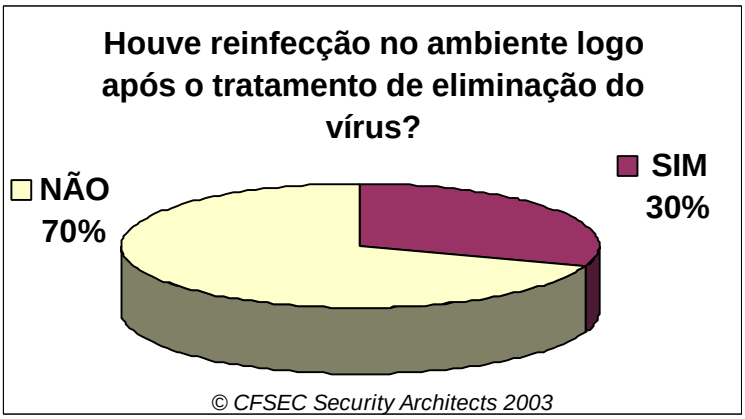


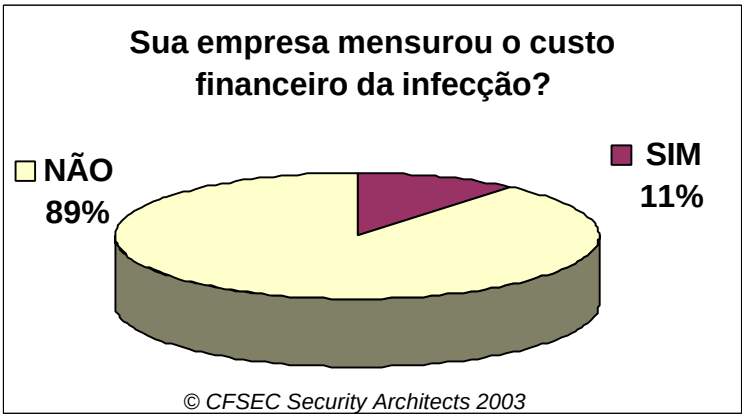
Continua...

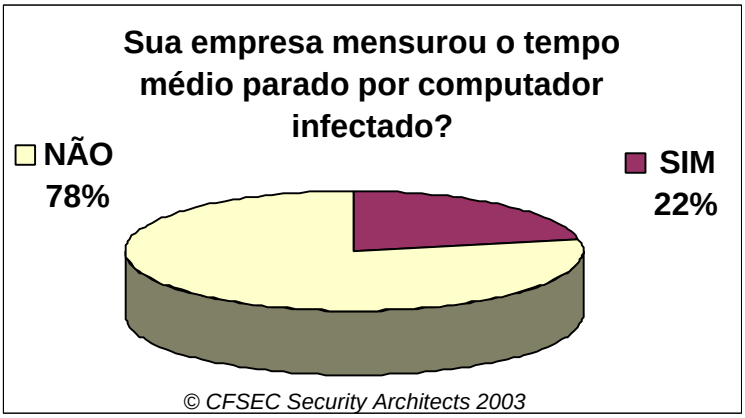
PESQUISA DO MÊS: … *continuação*.

Como você se relaciona com pragas eletrônicas?

Dentre os que responderam que já tinham sofrido algum tipo de infecção eletrônica neste ano, foram feitas mais três perguntas. Veja as respostas:







Segurança pelo mundo...

Virus no New York Times

Num editorial sóbrio, o The New York Times divide a culpa pela recente onda de vírus entre fabricantes, usuários e administradores, e lembra que o fato dos últimos vírus não serem destrutivos, deveria ser um alerta e não um alívio.

http://www.nytimes.com/2003/08/23/opinion/23SAT3.html

Nota da CFSEC: O editorial do The New York Times é apenas mais uma demonstração que a ineficiência no combate aos vírus de computador passou dos limites. O tratamento meramente tecnológico dado ao problema tende a gerar uma nova onda de problemas. Começam a se tornar cada vez mais comuns os emails falsos orientando os usuários a instalar supostas atualizações de antivírus e patches de sistema operacional que na verdade são vírus ou trojan. Em tempo, segundo vários jornais, o próprio NYT teve problemas com vírus recentemente: http://www.usatoday.com/tech/news/computersecurity/2003-08-22-nyt-offline_x.htm

Serviço de navegação anônima é grampeado

O site britânico The Register comenta matéria sobre a inserção de um mecanismo de "escuta" no sistema de navegação anônima JAP. A mudança foi feita segundo os responsáveis pelo serviço, devido à uma decisão judicial alemã.

http://www.theregister.co.uk/content/55/32450.html

Nota da CFSEC: O direito a privacidade na Internet ainda promete causar muita dor de cabeça. Não são poucos os exemplos de exageros. A pouca informação sobre o assunto e indefinição jurídica, fortalece o mal uso da tecnologia. Infelizmente, o abuso não é exclusividade do governo. Não são raros os casos de administradores de redes que abrem a caixa postal de seus usuários ou que espalham aos quatro ventos os sites acessados através do proxy da empresa, por determinado funcionário.

A novena dos patches

A edição norte americana da CSO Online traz em agosto uma excelente matéria sobre os benefícios e desastres causados pela aplicação de correções de segurança.

http://www.csoonline.com/read/080103/patch.html

Nota da CFSEC: A atualização de sistemas operacionais e aplicativos é sem dúvida alguma, um dos mais tradicionais processos de segurança corporativa. O artigo da CSO Online é preciso ao apresentar pontos normalmente esquecidos, como o teste dos patches e rollout nos demais servidores. Nós não acreditamos que exista alguma solução universal para o problema, mas apesar disso, acreditamos que a aplicação de patches é uma corrida obrigatoriamente perdida. O ciclo de descoberta e publicação de vulnerabilidades e patches é historicamente mais favorável aos invasores do que aos administradores. O patch é portanto apenas uma parte, diga-se de passagem importante, do processo de segurança como um todo. Diversas pragas eletrônicas poderiam ter sido evitadas sem uso de antivirus ou patches, mas ainda é raro encontrarmos processos de segurança suficientemente amadurecidos para isso.

Citibank alerta sobre fraude por email

Segundo a Agência Reuters, o Citibank informou aos seus correntistas norte-americanos a existência de uma fraude ocorrendo através da Internet. A fraude muito semelhante às brasileiras, solicita ao destinatário que acesse um site e informe o "Social Security number".

http://www.reuters.com/newsArticle.jhtml?type=internetNews&storyID=3297473

Nota da CFSEC: O problema com os spams de fraude ou "phishing" com vêm sendo chamados por alguns especialistas, é grave, e sua solução depende de educação e mudanças nos hábitos das empresas, que muitas das vezes são as verdadeiras culpadas pelo problema. O uso de correio eletrônico como ferramenta de marketing, proporcionou aos picaretas um grande universo de clientes a serem enganados. Das companhias aéreas aos home-brokers, passando por bancos e sites de comércio eletrônico. Até mesmo extrato bancário já foi legitimamente enviado através de executável. A situação é tão grave, que nem mesmo a assinatura digital através de S/MIME irá resolver. Tomando-se como exemplo os sites SSL que são falsificados diariamente, vemos que o que falta não é tecnologia e sim orientação aos clientes.

Informação ou desinformação?

Matéria da edição online da Folha de São Paulo afirma que terroristas usam criptografia e esteganografia para se comunicar secretamente pela Internet.

http://www1.folha.uol.com.br/folha/informatica/ult124u13745.shtml

Nota da CFSEC: Apesar de acreditar que o crime faz uso de técnicas de criptografia para proteger seus dados, nós questionamos até que ponto a fonte da Folha de São Paulo é segura. Conforme bem lembrou Bruce Schneier recentemente, em seu informativo, um relatório do governo norte-americano demonstra claramente que esse tipo de associação nem sempre é verdadeira. Em 2002, das 1358 escutas autorizadas pelos juízes federais americanos, apenas 16 continham alguma forma de criptografia.

http://www.counterpane.com/crypto-gram-0305.html

Infoguerra faz cobertura de simpósio de segurança

Adriano Cansian, docente da Unesp foi ao 12º Simpósio de Segurança da Usenix. "O simpósio reúne pesquisadores, administradores de sistemas, programadores, praticantes, e outros interessados nos últimos avanços na área de segurança em sistemas computadorizados."
http://www.infoguerra.com.br/infoguerra.php?newsid=1060303864,91785

Nota da CFSEC: O simpósio da Usenix é sem dúvida um dos mais importantes eventos da segurança da informação no mundo. O foco tecnológio/acadêmico do evento e os notáveis palestrantes fazem desse evento um prato cheio para os profissionais e acadêmicos da área. Para aqueles que não puderam participar do evento, o material pode ser lido no link abaixo (o site é fechado aos membros do Usenix):

http://www.usenix.org/publications/library/proceedings/sec03/tech.html

Serviço anti-spam sai do ar

O site de notícias Slashdot informou no último dia 27 o fim do serviço SPEWS oferecido pela Osirusoft. O serviço vinha sendo vítima de ataques de DDoS e processos movidos por indivíduos e organizações bloqueadas como spammers.

http://slashdot.org/article.pl?sid=03/08/27/0214238

Nota da CFSEC: Pelo visto, a briga pelo SPAM torna-se cada vez mais séria. A tecnologia, que já não era uma solução universal, torna-se cada vez mais ineficiente à medida em que os spammers se organizam. O problema é grave e só será solucionado quando governos e usuários da Internet decidirem tratar o problema de forma séria. No Brasil, a situação também é grave, mas pouca movimentação tem sido feita no sentido de inibir os transtornos causados pelo SPAM. Infelizmente, não costumamos nos lembrar que o custo do SPAM vem junto da conta do acesso a Internet que pagamos.

Polêmica sobre voto eletrônico continua nos EUA

Continua a polêmica em torno do sistema de votação eletrônica adotado por alguns estados norte americanos. Um jornal local de Atlanta, relata que após questionar a segurança do sistema de votações usado na Geórgia, uma programadora de 51 anos foi desafiada a provar suas afirmações de que poderia quebrar a segurança do sistema.

http://www.ajc.com/metro/content/metro/0803/23voting.html

Nota da CFSEC: Interessante observar que tanto no Brasil quanto nos EUA há paranóicos de plantão prontos a questionar aquilo que eventualmente é pregado como perfeito. Essa atitude é extremamente benéfica e fora alguns exageros dignos de séries de ficção científica, podemos dizer que a paranóia enriquece a democracia. É interessante notar que lá, assim como aqui, a impressão do voto está sendo usada como alternativa à desconfiança em torno do sistema 100% eletrônico. Ponto para nós brasileiros que já testamos a solução antes.

Hackers alemães descobrem nova forma para burlar biometria

Dois membros do Chaos Computer Club, renomado grupo de hackers alemães afirmaram ter descoberto uma forma de burlar sistemas de biometria baseados em impressões digitais. Ainda segundo a notícia, nenhum dos fabricantes contactados pelos hackers alemães responderam às solicitações de ambiente para teste.

http://www.securityfocus.com/news/6717

Nota da CFSEC: Apesar da polêmica em torno da originalidade do ataque apresentado pelos membros do Chaos Computer Club, há de se notar que novamente o hacking europeu destaca-se como uma corrente sensivelmente diferente do brasileiro e norte-americano. Lá, ao contrário daqui, hacking parece ser mais do que desfigurar sites. É importante notar também, que a recusa dos fabricantes em fornecer equipamentos para testes é nociva ao mercado de segurança. Fica cada vez mais claro que a obscuridade não é uma solução de marketing eficiente quando o assunto é segurança.

Yellow Security Paper

Derrapando na Largada
Dificuldades na adoção da ICP-Brasil

Por Augusto Paes de Barros, CISSP

Com a medida provisória 2200, em agosto de 2001, esperava-se que a adoção dos certificados digitais avançaria em alta velocidade. Porém, prestes a completar dois anos, a ICP-Brasil ainda não demonstra sinais de grande utilização. Os argumentos mais comuns são a demora nas definições e o alto custo das soluções de PKI. Existem outros fatores, entretanto, que podem trazer ainda mais impacto do que isso.

A ICP-Brasil define Práticas e Políticas de Certificação mínimas para qualquer AC que queira emitir certificados. Cada AC deve criar seus documentos baseados nestas versões mínimas. Ao analisarmos as DPCs (Declaração de Práticas de Certificação) e as PCs (Política de Certificação) das certificadoras já homologadas para funcionar encontramos diversos itens que podem dificultar a adoção dos certificados gerados por elas. Para podermos entender melhor o que são estas dificuldades, convém conhecermos alguns pontos destes documentos (mais precisamente das Políticas de Certificação):

- Titulares de Certificado
- Aplicabilidade
- Responsabilidade Financeira
- Suspensão e Revogação de Certificado

Através dos itens "Titulares de Certificado" e "Aplicabilidade" a PC indica quem pode ser titular dos certificados gerados e para que tipo de uso poderá utilizá-los. As ACs tem grande liberdade para apontar quem pode ser titular de seus certificados. A Caixa Econômica Federal, por exemplo, criou uma AC para uso operacional interno, e especificou que os certificados seriam gerados apenas para funcionários ou prestadores de serviço. No item de aplicabilidade, porém, a mesma PC segue o padrão mínimo da ICP-Brasil, que atesta que os certificados são válidos para utilização em "aplicações como confirmação de identidade na Web, correio eletrônico, transações on-line, redes privadas virtuais, transações eletrônicas, cifração de chaves de sessão e assinatura de documentos eletrônicos com verificação da integridade de suas informações".

Continua...

...continuação

Como podemos ver, não é especificado onde tais aplicações estão. Sendo assim, o certificado emitido pela “Autoridade Certificadora CAIXA para Uso Operacional Interno” pode ser usado em qualquer aplicação, dentro ou fora da Caixa. A resolução Nº7, que aprova os requisitos mínimos para as PCs, especifica que aplicações para o público em geral que aceitam certificados ICP-Brasil de um certo tipo, de uma certa AC, devem aceitar certificados do mesmo tipo emitidos por qualquer outra AC da ICP-Brasil.

Mas qual o problema? Esta “interoperabilidade” não é um dos motivos da criação da ICP-Brasil? O problema é que apenas o tipo de certificado (A1, A2, A3, A4, S1, S2, S3, S4) não é suficiente para que possamos decidir se o aceitamos ou não. Para entender melhor esta afirmação vamos analisar outros pontos existentes nas PCs, “Responsabilidade Financeira” e “Publicação e Repositório”. A definição das responsabilidades financeiras da AC SERPRO-SRF, uma das autorizadas em emitir os novos e-CPF, limita indenizações a 10 vezes o valor do certificado, ou seja, menos de mil reais. Tais certificados têm como um de seus usos autorizados a “Confirmação de identidade na Web”. Como uma empresa pode confiar em um sistema de autenticação, realizado por terceiros, que paga apenas mil reais caso seja comprovada a falha no processo de identificação? Quando um cartório reconhece a firma de uma pessoa em um comprovante de transferência de veículo, ele não limita os valores da transação para fins de indenização (na verdade, em um erro do cartório a responsabilidade financeira recai para o Estado, e não há limite de valor). Imagine o exemplo. Alguém “engana” um cartório e consegue reconhecer uma assinatura, supostamente sua, no documento de venda da sua Ferrari. Ela é passada para o nome de outra pessoa, e por uma fraude que era de responsabilidade do cartório evitar, você perdeu centenas de milhares de dólares. Quem deve assumir este prejuízo? Existe um limite para esta responsabilidade? Você ficaria tranqüilo em usar os serviços do cartório sabendo que há um limite para o valor das indenizações caso haja erro no processo?

Continua...

Leia este Yellow Security Paper na íntegra:

www.cfsec.com.br/artigos/ysp_0011.pdf