Amanda da Solidade Silva

De: Amanda da Solidade Silva em nome de Comissão Permanente de Licitação
Enviado em: quarta-feira, 6 de janeiro de 2021 18:06
Para: 'luciola.ferreira@inntecnologia.com'
Assunto: ENC: Resposta questionamento INN

Prezado licitante,

Segue a continuação das respostas ao questionamento realizado.

Atenciosamente,
Amanda
CPL

De: Marcelo Dias de Sá
Enviada em: quarta-feira, 6 de janeiro de 2021 18:05
Para: Comissão Permanente de Licitação <cpl@funasa.gov.br>
Cc: Darlan Henrique da Silva Venturelli <darlan.venturelli@funasa.gov.br>
Assunto: Resposta questionamento INN

Prezada CPL, segue a continuação das respostas.

4 - Em atenção aos itens 8.7.12. Deve possuir pelo menos 1 sensor para "escutar" o tráfego de rede de throughput de 1GB/s de análise e 8.7.24. Deve permitir o uso de portas espelhadas de switch (mirror port) para monitorar o tráfego e detectar potenciais riscos à Segurança; Entendemos que o sensor de análise de trafego pode ser considerado o próprio agente de endpoint uma vez que ele é responsável pela coleta e envio dos arquivos suspeitos. Está correto nosso entendimento?

Resposta 4: Entendimento incorreto.

5 – Em atenção ao item 8.7.16. Deve possuir a habilidade de detectar e analisar os seguintes protocolos e aplicativos: P2P, SMTP, POP3, IRC, DNS, HTTP, FTP, TFTP, SMB, MSN, AIM, YMSG, Yahoo Mail, Hotmail, RDP, DHCP, TELNET, File Transfer, VNC, Cisco-TELNET, Kerberos, DCE-RPC, SQL, HTTPS, SMB2, MMS, IMAP4, RTSP/RTP-UDP, RTSP/RTP-TCP, RTSP/RDT-UDP, RTSP/RDT-TCP, WMSP, SHOUTCast, RTMP, BiΣorent, Kazaa, Blubster, eDonkeyeMule, Gnucleus LAN, Gnutella/Limewire/Bearshare/Shareaza, Winny, WinMX, MLDonkey, DirectConnect, SoulSeek, OpenNap, Kuro, iMesh, Skype, Google Talk, Zultrax, Foxy, eDonkey, Ares, Miranda, Kceasy, MoodAmp, Deepnet Explorer, FreeWire, Gimme, GnucDNA GWebCache, Jubster, MyNapster, Nova GWebCache, Swapper GWebCache, Xnap, Xolox, Ppstream, AIM Express, Chikka SMS Messenger, eBuddy, ICQ2Go, ILoveIM Web Messenger, IMUniΘve, mabber, meebo, Yahoo Web Messenger, GPass, IP, ARP, TCP, UDP e IGMP; Entendemos que a ameaça avançada pode trafegar por sessões de redes e arquivos criptografados onde nunca serão analisados mesmos trafegando nestes protocolos e aplicações, uma vez que eles conseguem passar por este tipo de análise de trafego o único momento que realmente eles conseguem ser detectados seria no momento da de criptografia que acontece apenas no endpoint, considerando essa situação onde o existe analise do arquivo independente do protocolo e o modulo de controle de aplicação para bloqueio dessas aplicações indesejadas, estamos aderentes a proposta?

Resposta 5: O entendimento está incorreto.

Atenciosamente,