Conselho de Segurança debate riscos de ataques cibernéticos com ransomware

Órgão da ONU discutiu sequestro de aparelhos digitais como celulares e computadores até o pagamento de uma quantia exigida; OMS diz que número de ataques a hospitais e outros serviços de saúde aumentou em escala e frequência.

O Conselho de Segurança da ONU se reuniu nesta sexta-feira para debater as ameaças representadas por ataques cibernéticos contra hospitais e outras instalações e serviços de saúde.

O foco da discussão foi a utilização de “ransomware”, uma espécie de software usado para bloquear computadores, exigindo um resgate em dinheiro para desbloqueá-los.

Uma questão de vida ou morte

O diretor-geral da Organização Mundial da Saúde, OMS, citou dois exemplos de ataques deste tipo ao falar ao Conselho de Segurança.

Tedros Ghebreyesus ressaltou que essas ameaças cibernéticas em unidades de saúde “não são apenas questões de segurança e confidencialidade, elas podem ser questões de vida ou morte”.

O líder da OMS contou que em março de 2020, o Hospital Universitário de Brno, na República Tcheca, foi afetado por um ransomware que o forçou a desligar sua rede. Isso resultou na transferência de pacientes para instituições vizinhas e adiamento de procedimentos planejados.

Este episódio ocorreu quando a nação entrava em estado de emergência devido à pandemia de Covid-19.

Conselho de Segurança debate riscos de ataques cibernéticos com ransomware

OMS

Diretor-geral da OMS, Tedros Ghebreyesus

Serviços de radioterapia interrompidos

Tedros contou que em maio de 2021, o grupo criminoso Conti Ransomware comprometeu o sistema de saúde irlandês. O ataque começou com um e-mail contendo uma planilha como anexo, que quando aberta ativava o software malicioso.

O problema se espalhou por toda a rede durante dois meses, criptografando cerca de 80% dos dados e tornando a plataforma nacional de diagnóstico por imagem inacessível. Os serviços de radioterapia para pacientes com câncer tiveram que ser pausados em cinco grandes centros.

Como resultado, mais de metade dos hospitais adiaram consultas ambulatoriais e intervenções clínicas eletivas, com as equipes médicas recorrendo a processos baseados em papel para manter os serviços ativos.

Pagamento de resgate

O chefe da OMS explicou que estes ataques têm como alvo a infraestrutura digital das

instalações de saúde, visando derrubá-las. Para que o acesso seja devolvido, os criminosos exigem o pagamento de um resgate.

Os grupos de crimes cibernéticos operam com base na lógica de que quanto maior a ameaça à segurança dos pacientes, maior será o resgate que podem exigir.

Para restaurar o sistema e recuperar os dados rapidamente, as unidades de saúde muitas vezes estão dispostas a pagar valores altos, mesmo que não haja garantia de que os dados serão descriptografados e de que os invasores não tentarão novamente.

Tedros relatou estudos que mostram que os ataques ao setor da saúde aumentaram em escala e frequência.

Ocha/Ali Haj Suleiman
Uma médica trata um paciente com câncer

Cadeia biomédica também é alvo

Em inquérito global, realizado em 2021, mais de um terço dos entrevistados relataram pelo menos um ataque de ransomware no ano anterior. Deste total, 30% das vítimas “pagaram o resgate”.

No entanto, mesmo nesses casos, 31% dos entrevistados informaram que não recuperaram acesso aos seus dados criptografados.

Embora o foco principal dos ataques de ransomware sejam hospitais, a cadeia de abastecimento biomédica mais ampla também tem sido visada, incluindo laboratórios e empresas farmacêuticas.

Reforço na segurança cibernética

Tedros disse que para enfrentar esses desafios, a OMS e outras agências da ONU estão apoiando ativamente os Estados-membros com assistência técnica, normas, padrões e orientações para aumentar a resiliência das infraestruturas de saúde contra o cibercrime, incluindo ataques de ransomware.

Ele pediu que os países invistam em tecnologia e garantam que os orçamentos para projetos de saúde digital incluam os custos para mecanismos básicos de segurança cibernética.

O líder da OMS sugeriu ainda que os países colaborem em investigações conjuntas e aplicação da lei, compartilhar informações de inteligência e criando regionais redes para combater os criminosos.