Das motivações às consequências: O ataque à AMA e as dúvidas que ficam ‘no ar’

visao.pt/exameinformatica/noticias-ei/internet/2024-10-14-das-motivacoes-as-consequencias-o-ataque-a-ama-e-as-duvidas-que-ficam-no-ar

Francisca Andrade 14 de outubro de 2024

À medida que alguns serviços e plataformas da AMA voltam a estar disponíveis e que o incidente continua a ser acompanhado pelas autoridades, há dúvidas importantes que permanecem. Que consequências pode ter este incidente e o que fazer para manter a segurança neste momento?

Na última semana, a Agência para a Modernização Administrativa (AMA) confirmou que foi alvo de um ataque informático que causou disrupções na sua rede, com o acesso às suas plataformas e serviços a estar “preventivamente indisponível”. Embora não tenha feito referência ao tipo de ataque sofrido, o Centro Nacional de Cibersegurança (CNCS) deu conta de que foi notificado de um incidente de ransomware que comprometeu as infraestruturas geridas pela entidade e que teve um “impacto substancial” nos seus serviços.

Um dia após o ataque, a AMA avançou, em comunicado partilhado nas suas redes sociais, que “em virtude dos trabalhos realizados para reduzir os impactos do ataque informático” alguns serviços já se encontravam operacionais, o que permitiu o “restabelecimento progressivo do atendimento nas Lojas de Cidadão, bem como o acesso a outras plataformas e serviços digitais”.

Por outro lado, durante o fim de semana, o acesso a alguns serviços continuou condicionado. Como noticiado pelo jornal *Público*, a autenticação via Cartão de Cidadão, Chave Móvel Digital, número de utente ou número de telefone no Portal SNS 24 e respetiva aplicação esteve indisponível. Além disso, o envio de receitas médicas aos utentes através de SMS também foi afetado.

À medida que o incidente continua acompanhado pelas autoridades competentes, existem dúvidas importantes, sobretudo para os cidadãos, organizações e entidades que recorrem aos serviços e plataformas geridas pela AMA. Que consequências pode ter este incidente e o que fazer para manter a segurança neste momento?

Logo no seu último comunicado, a AMA deixava já um alerta: “ressalva-se que no caso de existirem eventuais contactos, através de qualquer canal, com pedidos de informações pessoais para recuperação de credenciais da Chave Móvel Digital, estes devem ser ignorados”.

À *Exame Informática,* Bruno Castro, fundador e diretor executivo da Visionware, explica que “em termos práticos, e visto que somos todos ‘interlocutores’ com a AMA, a probabilidade de virmos todos a ser alvos de ações de phishing – mais ou menos evoluídas – é extremamente elevada”.

Por esse motivo, “é fundamental que todos nós elevemos o nosso nível de alerta para possíveis tentativas de fraude via phishing ou outro método ainda mais evolutivo, até recorrendo a engenharia social”, realça.

Nas palavras do responsável, é também necessário aguardar que a AMA forneça informação mais detalhada sobre o sucedido e sobre que tipo de dados estarão em causa para “percebermos quais as possibilidades de ações maliciosas sobre todos nós”.

Em linha com Bruno Castro, David Russo, diretor executivo da Academia Nacional de Cibersegurança e CTO da CyberS3c.pt, afirma que “é importante aguardar por algum tipo de notificação e comunicação da própria AMA que esclareça que dados é que foram ao certo comprometidos”.

“Neste momento estamos a trabalhar sobre o desconhecido, como é normal em muitos ciberataques. O que deve ser feito é ter especial atenção a todos os serviços em que tenha usado a Chave Móvel Digital ou o Cartão de Cidadão ou qualquer aplicação relacionada”, destaca, acrescentando que é necessário ter igual cuidado com telefonemas de números desconhecidos e suspeitos.

Que consequências pode ter o ataque?

Embora possam assumir diferentes contornos, os ataques de ransomware caracterizam-se pela encriptação da informação presente num sistema após a infeção do mesmo, o que impossibilita o seu uso. Tipicamente, os atacantes pressionam as vítimas para pagarem um resgate, prometendo a recuperação de acesso ao sistema infectado.

Em muitos casos, além da encriptação de dados, os cibercriminosos exfiltram a informação que se encontra no sistema. “Tipicamente, é aqui onde o atacante tem a vantagem”, afirma David Russo. “A primeira consequência é mesmo a quebra da integridade e da confidencialidade da informação”.

“Os ciberataques de ransomware são altamente mediáticos e tipicamente muito destrutivos em todos os aspetos”, detalha Bruno Castro. A par das interrupções nas operações e do roubo de dados de uma organização, outra consequência deste tipo de ataque é a “eventualidade de um comprometimento da integridade dos dados armazenados”, o que pode colocar em risco a informação pessoal e confidencial tanto de colaboradores como parceiros e clientes.

“A situação torna-se particularmente grave no caso do roubo de dados, pois pode implicar também a sua divulgação ou comercialização na comunidade criminosa, que poderá utilizar essa informação para gerar outros vetores maliciosos ou ações de fraude no ecossistema da organização”, realça o responsável. A tudo isto, e “sem garantia da total recuperação”, somam-se ainda os custos associados à resposta a um incidente deste tipo, seja a nível financeiro, legal e mediático.

De modo geral, “qualquer ciberataque com sucesso, seja numa entidade governamental, pública ou do sector privado, acabará sempre por ter consequências”, aponta Bruno Castro. Aqui o impacto nas operações pode variar quanto à gravidade, no entanto, “as consequências em termos mediáticos e reputacionais acabam por estar presentes, ainda que, de forma mais ou menos direta”.

No que respeita aos incidentes que envolvem entidades governamentais, que “têm um compromisso acrescido de garantir a confiança e proteção da informação de todos os seus cidadãos”, estes casos, “pela sua dimensão e sensibilidade, podem criar falta de confiança e levantar questões emergentes sobre uma eventual insuficiência de investimento em cibersegurança e ciberdefesa a nível do Estado”, indica. “Cria naturalmente uma sensação de insegurança junto da sociedade no que respeita à capacidade e maturidade em cibersegurança do Estado Português”.

Motivações políticas ‘no ar’?

Numa altura em que, em Portugal, as atenções se têm centrado na política, com foco na proposta de Orçamento de Estado para 2025, um incidente que envolve uma entidade como a AMA pode deixar ‘no ar’ questões sobre as verdadeiras motivações do ataque. No entanto, os especialistas consultados pela *Exame Informática*, afastam, para já, um cenário de ataque com motivações políticas.

Bruno Castro explica que “normalmente, as motivações por detrás de um ciberataque, nomeadamente quando envolve a tipologia de ransomware, são essencialmente financeiras”. “Não nos podemos esquecer que o cibercrime está assente num modelo de negócio ultra maduro que tem como mote atacar organizações para gerar ‘dinheiro’ em benefício próprio”, afirma.

É certo que um ciberataque a uma entidade governamental “tem o potencial de colocar em causa a confiança da sociedade civil no nível de maturidade e segurança das nossas instituições públicas”. Além disso, “a AMA pela sua exposição, volume de dados envolvidos e criticidade da sua atividade, preenche o perfil típico do cibercrime para ações de ransomware”. No entanto, o responsável defende que nesta fase, ainda é cedo para apontar uma explicação motivacional clara para o caso.

Já David Russo aponta para a possibilidade de ter sucedido algo já visto em múltiplos incidentes anteriores de ransomware, o que descreve como um “ataque de arrastão”. Estes são casos em que os atacantes recorrem a software concebido para explorar vulnerabilidades numa rede. Ao encontrar uma máquina que corresponda à vulnerabilidade que os cibercriminosos pretendem afetar, este software desencadeia toda uma série de ações para a explorar e, por consequência, ativar o ransomware.

“A maioria do ransomware é um ataque de arrastão, ou seja, houve a infelicidade de uma máquina ter uma vulnerabilidade e essa rede não estar resiliente o suficiente ou de aquela parte da rede ter sido comprometida”, indica o responsável.

Trabalhar a resiliência

O ransomware é uma ameaça conhecida para as organizações, mas a sua evolução implica uma constante necessidade de aumentar não só a resiliência e a segurança, mas também a resposta a incidentes, defende David Russo. Para tal, há todo um conjunto de mecanismos que têm de funcionar em harmonia.

“As organizações têm de assegurar que fazem regularmente rotinas de inspecção”, que validam se têm ou não vulnerabilidades, se têm planos de correção e gestão de falhas de segurança, assim como planos bem definidos de gestão de risco e de continuidade de negócio, sem esquecer se têm os seus backups em dia. “Há aqui outra situação que é muito importante nas organizações que é trabalhar com sistemas XDR (Extended Detection and Response)”, aponta também o responsável.

“É impossível, de alguma forma, assentarmos toda a segurança de uma organização num só ponto. Isto tem de ser um trabalho conjunto entre as pessoas, processos e tecnologia”, realça. “Tem de existir um bom processo preparativo, um processo proativo e um processo de resposta. Isto é, nada mais, nada menos, do que um conjunto de etapas que têm de ser feitas e isto demora tempo e tem de ter o seu investimento”.