IoT, autenticação e serviços em nuvem impulsionam aumento expressivo na adoção de ICPs e no volume de certificados, aponta nova pesquisa da Entrust

Estudo Anual de Tendências de ICP e IoT encontra níveis sem precedentes de desafios, mudanças e incertezas da ICP em 2020

São Paulo, 13 de outubro de 2020 – As organizações estão aumentando rapidamente o tamanho, o escopo e a escala de sua infraestrutura de proteção de dados, refletidos em aumentos expressivos na adoção de Infraestrutura de Chaves Públicas (ICP) em empresas em todo o mundo, de acordo com novas pesquisas da Entrust. A ICP está no centro de quase todas as infraestruturas de TI, permitindo a segurança para iniciativas digitais críticas, como nuvem, implantação de dispositivos móveis, identidades e internet das coisas (IoT).

O Estudo Anual de Tendências Globais ICP e IoT de 2020, realizado pela empresa de pesquisa Ponemon Institute e patrocinado pela nCipher Security, uma empresa Entrust, é baseado no feedback de mais de 1.900 profissionais de segurança de TI em 17 países.

IoT, autenticação e nuvem são os principais drives no crescimento da adoção de ICPs

À medida que as organizações se tornam mais dependentes de informações digitais e enfrentam ataques cibernéticos cada vez mais sofisticados, dependem da ICP para controlar em grande escala o acesso aos dados e verificar as identidades de pessoas, sistemas e dispositivos.

A IoT é a tendência de crescimento mais rápido e que impulsiona a implantação de aplicações ICP, subindo 26% nos últimos cinco anos e para 47% em 2020, com os serviços baseados em nuvem como o segundo driver mais alto citado por 44% dos entrevistados.

O uso da ICP aumenta nos casos de uso de nuvem e autenticação

Os certificados TLS/SSL para sites e serviços voltados ao público são o caso de uso mais citado para credenciais ICP (84% dos entrevistados). As aplicações baseadas em nuvem pública tiveram o crescimento mais rápido em relação ao ano anterior, com 82%, um aumento de 27% em relação a 2019, seguido pela autenticação de usuários corporativos em 70% dos entrevistados, um aumento de 19% em relação a 2019. Todos ressaltam a necessidade crítica da ICP no suporte a aplicações corporativas principais.

O número médio de certificados que uma organização precisa gerenciar cresceu 43% no estudo de 2020 em relação ao ano anterior, de 39.197 para 56.192 certificados, destacando um requisito fundamental para a gestão de certificados corporativos. O aumento provavelmente é impulsionado pela transição do setor para períodos de validade de certificados mais curtos e pelo crescimento acentuado nos casos de uso de usuários de nuvem e de usuários corporativos.

Desafios, mudanças e incertezas

O estudo de 2020 constatou que os profissionais de segurança de TI enfrentam novos desafios para permitir que as aplicações utilizem ICP. Mais da metade (52%) citou a falta de visibilidade das capacidades de segurança existentes na ICP como seu principal desafio, um aumento de 16% em relação ao estudo de 2019. Essa questão ressalta a falta de experiência em segurança cibernética disponível até mesmo nas organizações mais bem preparadas e a necessidade de especialistas em ICP que possam criar roteiros corporativos personalizados com base nas melhores práticas de segurança e operacionais. Os entrevistados também citaram a incapacidade de alterar aplicações legadas e a incapacidade das ICPs existentes de suportar novas aplicações como desafios críticos – ambos em 51%.

Quando se trata de implantar e gerenciar uma ICP, os profissionais de segurança de TI são os mais desafiados por questões organizacionais, como nenhuma propriedade clara, habilidades e recursos insuficientes. Os números de implantação da ICP no estudo indicam claramente uma tendência para abordagens mais diversificadas, com as ofertas como serviço se tornando ainda mais prevalentes do que as ofertas presenciais em alguns países.

As duas maiores áreas de mudança e incerteza da ICP vêm de novas aplicações, como IoT (52% dos entrevistados) e mandatos e padrões externos (49%). O ambiente regulatório também está impulsionando cada vez mais a implantação de aplicações que usam ICPs, citados por 24% dos entrevistados.

As práticas de segurança não acompanharam o crescimento

Nos próximos dois anos, uma média de 41% dos dispositivos IoT dependerão principalmente de certificados digitais para identificação e autenticação. A criptografia para dispositivos IoT, plataformas e repositórios de dados está em apenas 33% – um potencial ponto de exposição para dados confidenciais. Os entrevistados citaram várias ameaças à segurança de IoT, incluindo alterar a função de dispositivos IoT por malwares ou outros ataques (68%) e controle remoto de um dispositivo por um usuário não autorizado (54%). No entanto, os respondentes classificaram os controles relevantes para a proteção contra malware – como fornecer patches e atualizações com segurança para dispositivos IoT – em último item de uma lista dos cinco recursos de segurança de IoT mais importantes.

O Instituto Nacional de Padrões e Tecnologia dos EUA (NIST) recomenda que módulos criptográficos para autoridades certificadoras (CAs), servidores de recuperação-chave e respondentes OCSP devem ser validados para o nível 3 ou superior do FIPS 140-2. Trinta e nove por cento dos entrevistados neste estudo usam módulos de segurança de hardware (HSMs) para proteger suas ICPs, na maioria das vezes para gerenciar as chaves privadas para suas CAs raiz, emissão ou política. No entanto, apenas 12% dos entrevistados indicam o uso de HSMs em suas instalações OSCP, demonstrando uma diferença significativa entre as melhores práticas e as práticas observadas.

"A ICP sustenta a segurança tanto do mundo dos negócios quanto para os consumidores, desde a assinatura digital de transações e aplicações para provar a fonte, passando pela integridade, até apoiar a autenticação de smartphones, consoles de jogos, passaportes, bilheteria de transporte coletivo e

mobile banking", diz Larry Ponemon, fundador do Instituto Ponemon. "O Estudo Anual de Tendências Globais de ICP e IoT de 2020 mostram um aumento no uso de credenciais ICP para aplicações baseadas em nuvem e autenticação de usuários corporativos, ressaltando a criticidade da ICP no suporte a aplicações corporativos principais."

"Observamos uma crescente dependência da ICP justaposta com discussões de equipes internas para adaptá-la às novas necessidades do mercado, impulsionando mudanças nos modelos e métodos tradicionais de implantação da ICP", diz John Grimm, vice-presidente de estratégia para soluções digitais da Entrust. "Em áreas mais novas como a IoT, as empresas vêm falhando em priorizar mecanismos de segurança, como a assinatura de firmware que neutralizariam as ameaças mais urgentes, como o malware. E com o aumento maciço de certificados emitidos e adquiridos encontrados no estudo deste ano, a importância do gerenciamento automatizado de certificados, uma abordagem flexível de implantação de ICPs e uma forte segurança baseada em práticas recomendadas, incluindo HSMs, nunca foi tão grande."

Infraestrutura de Chave Pública e IoT no Brasil

- 80% dos entrevistados favorecem o modelo interno de ACs (Autoridades Certificadoras) mais do que qualquer outro país (a média global é 60%), e fazem menos uso de ACs gerenciadas hospedadas externamente (20% no Brasil versus a média global de 43%)
- 42% usam ACs raiz offline, uma prática recomendada de ICP, mais do que qualquer outro país (a média global é 28%)
- Possui o menor número de especialistas em ICP entre todos os países (34% não contam com especialistas versus a média global de 24%)
- Uso extremamente baixo (menor de todos os países) de HSMs para ACs online e emissão de ACs (16% para cada um, contra 36% e 42% médias globais)
- Menor previsão de uso entre todos os países de certificados digitais para dispositivos IoT nos próximos 2 anos (30% versus 41% da média global)
- Avaliam a descoberta de dispositivos o maior de todos os recursos de segurança IoT em comparação com os outros países (4,7 de 5, contra 3,3 média global)
- Os entrevistados brasileiros relataram que tanto os celulares de consumo quanto a IoT são as tendências mais importantes que impulsionam a implantação de aplicações para o uso de ICPs (49% e 50% respectivamente)

Recurso para download: Estudo Global de Tendências ICP e IoT de 2020

Metodologia global de estudo de tendências ICP e IoT trends 2020

O Estudo Anual de Tendências Globais de ICP e IoT de 2020 captura o estado atual da maturidade e, os desafios da ICO, além da influência da IoT nas tendências para as ICPs. O relatório resume o quinto resultado anual de uma pesquisa concluída por 1.934 profissionais de segurança de TI nos seguintes 17 países/regiões: Austrália, Brasil, França, Alemanha, Hong Kong, Índia, Japão, México, Oriente Médio

(Arábia Saudita e Emirados Árabes Unidos), Holanda, Federação Russa, Coreia do Sul, Sudeste Asiático (Indonésia, Malásia, Filipinas, Tailândia e Vietnã), Suécia, Taiwan, Reino Unido e Estados Unidos.

O estudo de 2020 é o quinto relatório anual sobre tendências globais de ICP e IoT, patrocinado pela nCipher Security, uma empresa da Entrust, e líder no mercado de módulos de segurança de hardware (HSM) de uso geral, capacitando organizações líderes mundiais, fornecendo confiança, integridade e controle para suas informações e aplicações críticas para os negócios.

Sobre a Entrust

A Entrust mantém o mundo em movimento seguro, permitindo identidades, pagamentos e proteção de dados confiáveis. Hoje, mais do que nunca, as pessoas exigem experiências perfeitas e seguras, seja cruzando fronteiras, fazendo uma compra, acessando serviços do governo eletrônico ou fazendo login em redes corporativas. A Entrust oferece uma amplitude incomparável de soluções de segurança digital e emissão de credenciais no centro de todas essas interações. Com mais de 2.500 colegas, uma rede de parceiros globais e clientes em mais de 150 países, não é de admirar que as organizações mais confiadas do mundo confiem em nós. Para saber mais visite www.entrust.com.

Contatos para a imprensa:
Talquimy
Alessandra Neris - (11) 99104-4938 – atendimento@talquimy.com.br