Technology Leadership Council Brazil

IBM Academy of Technology Affiliated

Mini Paper Series Ano 14
Dezembro, 2018 – Nº 326

Pervasive Encryption – nova criptografia em mainframe

Eugênio Fernandes

Dado é o novo perímetro. Para entendermos o alcance dessa frase, devemos lembrar o quanto é gasto para a proteção do ambiente de Tecnologia da Informação (TI), como firewall, infraestrutura, gerência de identidade, entre outros. Onde se devem concentrar os esforços? Deve-se impedir que entre no castelo ou que roubem as joias da coroa? A informação é a parte mais sensível do processamento de dados e é nela que devemos concentrar os esforços de proteção.

O sistema mainframe alterou o paradigma de segurança quando possibilitou *Pervasive Encryption* em julho de 2017, no lançamento da nova máquina IBM z14. Na prática, essa facilidade está disponível em outros modelos de máquina, mas vale lembrar que o desempenho na z14 é significativamente superior aos anteriores, sendo sete vezes mais rápida que na z13. O modelo z196 é o hardware mínimo para *Pervasive Encryption*, assim como o Sistema Operacional mínimo é o zOS 2.2 (ou 2.1, em regime de tolerância, ou seja, dados criptografados podem ser lidos, mas não gerados).

Pervasive Encryption, através do uso de chaves protegidas (*Protected Keys*), adiciona um novo nível de acesso, além dos já conhecidos pelo Resource Access Control Facility (RACF): *None*, *Read*, *Update*, *Control* e *Alter*. Um acesso *Update* ou maior, que antes possibilitava a leitura integral do dado, hoje necessita também ter disponibilizada a chave de leitura, sem a qual o dado estará criptografado. O usuário com acesso *Alter*, por exemplo, poderá mover o dado, atualizá-lo e deletá-lo, mas não poderá lê-lo. Com isso, usuários de serviço, que realizam backup, movimentação e tratamento de dados, não serão capazes de acessar a informação. Como funcionava antes da *Pervasive Encryption*? Esse perfil de usuário podia ler dados sensíveis, mas "não deveria". Possibilidade considerada péssima, em termos de auditoria e segurança.

Onde se definem os acessos aos dados? O conceito de *Protected Key*, com processamento na *CP Assist for Cryptographic Functions* (CPACF), possibilita alto desempenho (em contrapartida à *Secure Key*, processada no Crypto Express 6S, utilizada para sistema de pagamentos com cartão, com PIN e chip) e alta segurança (em comparação à *Clear Key*, armazenada em branco). Associa-se um grupo de arquivos a uma *key label* e essa associação ocorre, nesta ordem, em (1) definições no RACF, (2) definições temporárias no JCL, IDCAMS, TSO Allocate ou alocação dinâmica ou ainda (3) no SMS. Dessa maneira, um arquivo ou grupo de arquivos já nasce com criptografia definida, bem como sua lista de acessos. Não há mais o diálogo constante entre o dono da aplicação e o gestor da criptografia. No mesmo conceito da alocação de *storage* por novos arquivos, via SMS, a criptografia ocorre por parâmetros definidos na lista acima (RACF, SMS e outros). Um arquivo é criptografado "ao nascer", sem dependência de processo adicional.

Para terminar, listamos os principais conceitos que devem estar associados à *Pervasive Encryption*: (1) Dados são criptografados em repouso (*at rest*), ou seja, são processados em claro (para criptografia de dados em memória de base de dados DB2 ou IMS, outros produtos devem ser utilizados, como o Security Guardium Data Encryption); (2) Aplicações não necessitam ser alteradas; (3) Arquivos podem ser criptografados sem necessidade de parada de aplicativos para DB2, IMS DB e zFS (VSAM e arquivos sequenciais necessitam de parada dos aplicativos); (4) Somente arquivos com *Extended Format* (sequenciais ou VSAM) podem ser criptografados; (5) Se necessário, compactar arquivos antes da criptografia, para máximo aproveitamento de espaço; (6) A criptografia é realizada em massa, com alto *throughput*; (7) zVM e Linux no mainframe também podem utilizar *Pervasive Encryption*; (8) Utiliza padrão de criptografia AES-256; (9) Registros de System Management Facilities (SMF) são gravados para fins, principalmente, de auditoria, indicando arquivos criptografados ou não, bem como acesso a eles; (10) Por meio do IBM Security zSecure é fornecido administração, auditoria, alertas e *enforcement* para uso de *Pervasive Encryption*.

Em resumo, *Pervasive Encryption* protege dados por políticas de segurança para evitar alterações custosas em aplicativos. O dado é o novo perímetro.

Para saber mais

Redbook: ***https://ibm.biz/BdYQL8***

Badge para Pervasive Encryption: ***https://ibm.biz/BdYQuq***

Documentação de Data Encryption: ***https://ibm.biz/BdYQwW***

Estimativa de Uso de Recursos (zBNA): ***https://ibm.biz/BdYQUU***

Eugênio Fernandes é IT Specialist, consultor de segurança para mainframe para América Latina, com 33 anos de experiência em tecnologia de informação, formado em Engenharia Mecânica pela Escola de Engenharia Mauá e membro do TLC-BR desde 2007 e da AoT desde 2017. O **Mini Paper Series** é uma publicação quinzenal do **TLC-BR** e para assinar e receber eletronicamente as futuras edições, envie um e-mail para **tlcbr@br.ibm.com**.