MÃ HÓA TRONG WINDOWS VISTA CHƯA PHẢI 'THUỐC TRỊ BÁCH BỆNH'

Microsoft đã trang bị thêm một số chức năng bảo mật cho hệ điều hành thế hệ mới, trong đó có Bitlocker. Kỹ thuật mã hóa ổ cứng này có thể đóng vai trò quan trọng trong doanh nghiệp nhưng còn tồn tại nhiều hạn chế, do đó thị trường vẫn cần đến các giải p

Microsoft đã trang bị thêm một số chức năng bảo mật cho hệ điều hành thế hệ mới, trong đó có Bitlocker. Kỹ thuật mã hóa ổ cứng này có thể đóng vai trò quan trọng trong doanh nghiệp nhưng còn tồn tại nhiều hạn chế, do đó thị trường vẫn cần đến các giải pháp an ninh khác. Bitlocker, trước có tên "Secure Startup - Full Volume Encryption", mang lại cho người dùng khả năng mã hóa toàn bộ ổ cứng, tức tiến xa hơn kỹ thuật mã hóa tệp tin Encrypting File Sytem trong Windows 2000 và XP. Kết hợp với công nghệ Trusted Platform Module (TPM), chức năng này giúp người sử dụng phòng ngừa trường hợp máy tính chứa thông tin quan trọng bị mất cắp hoặc thất lạc và tránh bị truy cập trái phép. Phương pháp trên bắt nguồn từ kỹ thuật bảo mật Palladium, sau được Microsoft đổi tên thành Next Generation Secure Computing Base (Cơ sở điện toán bảo mật thế hệ mới). Nguyên tắc hoạt động Bitlocker được gắn trong các phiên bản "Enterprise", "Ultimate" và "Longhorn" của Windows Vista. Để sử dụng được chức năng TPM, bo mạch chủ cần có chip bảo mật tương ứng chuẩn 1.2 của công ty Trusted Computing Group. Quá trình mã hóa Vista không diễn ra tự động mà phải được người dùng kích hoạt. Chip TPM chỉ cần thiết trong lúc khởi động máy tính để kiểm tra tính nguyên vẹn của hệ thống. Bitlocker sẽ sử dụng khả năng tạo trị băm cho chương trình của TPM. Thông qua việc so sánh giá trị băm hiện hành với giá trị được xác định ban đầu, chương trình đó có thể nhận biết BIOS và tệp tin hệ thống (loader file) đã bị biến đổi hay chưa. Bên cạnh đó, Microsoft dùng chip TPM để đảm bảo những cá nhân nhất định mới được phép tiếp cận dữ liệu. Khâu mã hóa nội dung ổ cứng được tiến hành nhờ một khóa do Bitlocker tạo ra và được lưu trong chip TPM. Khi người sử dụng khởi động máy tính, hệ điều hành sẽ tự động đọc khóa này và cho phép truy cập dữ liệu. Vì thế, người dùng sẽ không thể xem thông tin nếu mang ổ cứng sang máy khác. Khóa này cũng có thể được lưu trữ trong thẻ nhớ USB. Lúc khởi động, hệ điều hành sẽ tìm xem thẻ nhớ có được gắn vào máy tính hay không. Sử dụng khóa này kết hợp với số định dạng cá nhân (PIN) sẽ nâng cao khả năng bảo mật. Nhờ chức năng "anti-hammering" của TPM, sau mỗi lần nhập PIN sai, thời gian chờ giữa hai lần nhập liệu sẽ tăng gấp đôi. Như thế, người ta sẽ phải đợi nhiều ngày mới có thể thực hiện lại sau 20 lần nhập sau. Đánh giá của chuyên gia Nobert Pohlmann, giáo sư của Viện Bảo mật Internet thuộc Đại học thực hành Gelsenkirchen (Đức), đánh giá cao quyết định tích hợp trực tiếp các kỹ thuật bảo mật như Bitlocker vào trong sản phẩm của Microsoft. Pohlmann tin rằng phần mềm này sẽ đóng vai trò rất quan trọng trong các doanh nghiệp lớn và các nhà cung ứng giải pháp bảo mật sẽ mất thị phần vì Bitlocker. Tuy nhiên, công ty Yankee Group lại không tán thành nhận định này. Trong báo cáo "Vista sẽ không thể 'kết liễu' thị trường bảo mật Windows" (Microsoft's Vista won't stop the Windows Security Aftermarket), Yankee dự đoán rằng Bitlocker/Vista chỉ sẽ làm giảm nhẹ nhu cầu cần dùng công cụ bảo mật khác từ nhà sản xuất thứ ba. Theo đánh giá của Richard Aufreiter, Giám đốc sản phẩm bảo mật của hãng Utimaco, Bitlocker chỉ thay thế được "một phần các chức năng" so với phiên bản Safeguard Easy của Utimaco. Nó có thể mã hóa được phân vùng khởi động của máy tính, nhưng lại không hỗ trợ các phương tiện lưu trữ dữ liệu khác. "Vì thế, chúng tôi sẽ đón nhận phần mềm của Microsoft một cách bình thản, ít nhất là trong giai đoạn đầu", Aufreiter nói. Phan Ba