

TĂNG CƯỜNG BẢO MẬT DỮ LIỆU TRONG KẾ TOÁN THÔNG QUA ỨNG DỤNG CÔNG NGHỆ SỐ

● NGUYỄN QUANG HƯNG

Khoa Kế toán Kiểm toán,
Trường Đại học Kinh tế - Kỹ thuật công nghiệp

TÓM TẮT:

Bài viết phân tích các rủi ro chính về bảo mật dữ liệu trong lĩnh vực kế toán, từ đó đề xuất những giải pháp hiện đại như ứng dụng AI, blockchain và các công nghệ tự động hóa. Mục tiêu nhằm giúp doanh nghiệp tăng cường bảo vệ thông tin tài chính trước những mối đe dọa khó lường trong thời đại số. Đồng thời, bài viết nhấn mạnh tầm quan trọng của việc xây dựng một chiến lược bảo mật toàn diện để giảm thiểu tổn thất và gia tăng niềm tin của khách hàng.

Từ khóa: bảo mật dữ liệu, kế toán, AI, blockchain, an toàn thông tin.

1. Đặt vấn đề

Trong bối cảnh chuyển đổi số ngày càng mạnh mẽ, bảo mật dữ liệu trở thành mối quan tâm hàng đầu trong lĩnh vực kế toán. Các hệ thống tài chính chứa lưu lượng lớn thông tin nhạy cảm, từ báo cáo tài chính, hóa đơn điện tử đến dữ liệu khách hàng. Sự gia tăng của các cuộc tấn công mạng, rò rỉ thông tin và nguy cơ gian lận nội bộ đặt ra thách thức không nhỏ cho các doanh nghiệp. Theo Báo cáo Điều tra An ninh mạng Toàn cầu 2023 của PwC, hơn 60% các công ty tài chính trên toàn thế giới đã ghi nhận sự gia tăng các cuộc tấn công mạng trong vòng 2 năm qua. Đặc biệt, những lỗ hổng trong quy trình kế toán thủ công và việc phụ thuộc vào các hệ thống truyền thống khiến doanh nghiệp dễ bị tổn thương hơn bao giờ hết. Trước thực trạng đó, nhu cầu áp dụng các giải pháp hiện đại như AI, blockchain và tự động hóa trở nên bắt buộc. AI giúp phát hiện những hành vi đáng ngờ thông qua phân tích dữ liệu thời gian thực, trong

khi blockchain đảm bảo tính minh bạch và không thể sửa đổi của dữ liệu. Việc áp dụng các giải pháp này không chỉ tăng cường an toàn thông tin mà còn giúp doanh nghiệp nâng cao độ tin cậy và hiệu quả quản lý. Hơn nữa, các quy định pháp lý ngày càng nghiêm ngặt về bảo mật thông tin tài chính cũng tạo áp lực cho các tổ chức phải cải thiện hệ thống bảo mật, qua đó thúc đẩy việc đổi mới và ứng dụng công nghệ hiện đại. Chính vì thế, việc nhận diện các rủi ro và tìm ra giải pháp bảo mật tiên tiến trong kế toán không chỉ là vấn đề cấp bách mà còn là yếu tố sống còn cho sự phát triển bền vững của doanh nghiệp.

2. Bảo mật dữ liệu trong kế toán

2.1. Tình hình bảo mật dữ liệu trong kế toán

Trong bối cảnh chuyển đổi số và sự phát triển của công nghệ, lĩnh vực kế toán đang đối mặt với nhiều thách thức liên quan đến bảo mật dữ liệu. Sự gia tăng nhanh chóng của các giao dịch điện tử và việc số hóa các quy trình kế toán không chỉ mang

lại tiện ích mà còn tạo ra nhiều lỗ hổng tiềm ẩn. Theo Báo cáo Rủi ro Toàn cầu 2022 của Diễn đàn Kinh tế Thế giới (WEF), các vụ tấn công mạng vào hệ thống tài chính chiếm tới 39% tổng số các vụ vi phạm bảo mật dữ liệu trên toàn cầu. Đặc biệt, trong giai đoạn đại dịch Covid-19, khi hình thức làm việc từ xa trở nên phổ biến, nhiều doanh nghiệp đã không kịp thời nâng cấp hệ thống bảo mật, tạo cơ hội cho tin tặc xâm nhập.

Ngoài ra các khảo sát gần đây cũng chỉ ra rằng nhiều doanh nghiệp chưa nhận thức đầy đủ về mức độ nghiêm trọng của các rủi ro bảo mật dữ liệu trong kế toán. Theo Khảo sát An ninh mạng của IBM năm 2021, 45% các tổ chức tài chính cho biết họ chưa có kế hoạch cụ thể để đối phó với các mối đe dọa an ninh mạng. Điều này làm gia tăng nguy cơ mất dữ liệu và thiệt hại tài chính đáng kể.

Một ví dụ điển hình là vụ tấn công mạng vào Công ty kế toán Deloitte năm 2017, khi tin tặc xâm nhập vào hệ thống email và đánh cắp hàng loạt thông tin nhạy cảm của khách hàng. Nguyên nhân chính là do việc bảo mật kém và không áp dụng xác thực hai yếu tố (2FA). Sự cố này đã làm tổn hại nghiêm trọng đến uy tín của Deloitte và còn khiến công ty này phải chi hàng triệu USD cho các biện pháp khắc phục và bồi thường.

Không chỉ dừng lại ở các mối đe dọa bên ngoài, rủi ro từ bên trong doanh nghiệp cũng là một vấn đề đáng lo ngại. Nhiều trường hợp gian lận nội bộ xảy ra do thiếu cơ chế kiểm soát chặt chẽ và sự phụ thuộc quá lớn vào các quy trình thủ công. Một nghiên cứu của Hiệp hội Kế toán Công chứng Anh quốc (ACCA) vào năm 2020 cho thấy, 27% các vụ gian lận tài chính trong doanh nghiệp có liên quan trực tiếp đến nhân viên nội bộ.

Do đó, bảo mật dữ liệu trong kế toán không chỉ dừng lại ở việc bảo vệ các số liệu tài chính, mà còn bao gồm các thông tin nhạy cảm như dữ liệu khách hàng, các hợp đồng, chi tiết thuế và thông tin chi trả. Trong trường hợp những dữ liệu này bị rò rỉ hoặc bị tấn công, không chỉ làm giảm sự tin tưởng của khách hàng, mà còn có thể vi phạm các quy định bảo mật của các cơ quan quản lý và gây ra những vấn đề pháp lý nghiêm trọng. Do đó, bảo

mật trong kế toán không chỉ là vấn đề của công nghệ, mà còn là vấn đề của quy trình và nhân sự.

2.2. *Hậu quả của việc rò rỉ dữ liệu*

Rò rỉ dữ liệu là một trong những mối đe dọa lớn nhất đối với các tổ chức và doanh nghiệp trong mọi lĩnh vực, đặc biệt là trong các ngành như tài chính, ngân hàng và kế toán. Theo báo cáo "Data Breach Investigations Report 2023" của Verizon, có đến 82% các cuộc tấn công mạng liên quan đến việc rò rỉ thông tin và 49% trong số đó là các cuộc tấn công do các hacker có chủ đích nhằm lấy cắp dữ liệu.

Hậu quả của việc rò rỉ dữ liệu có thể rất nghiêm trọng và đa dạng, từ việc làm giảm niềm tin của khách hàng đến việc đối mặt với các yêu cầu kiện tụng và các hình phạt pháp lý. Theo báo cáo "Cost of a Data Breach Report 2023" của IBM, các tổ chức bị rò rỉ dữ liệu thường phải chịu các khoản chi phí lớn liên quan đến việc điều tra, khắc phục sự cố và bồi thường cho khách hàng bị ảnh hưởng. Việc mất dữ liệu nhạy cảm như thông tin tài khoản ngân hàng, số thẻ tín dụng, hay các thông tin cá nhân quan trọng có thể dẫn đến việc khách hàng bị thiệt hại trực tiếp hoặc bị mất tiền.

Ngoài các hậu quả tài chính, việc rò rỉ dữ liệu còn có thể làm giảm sự tin nhiệm của công ty đối với khách hàng và đối tác. Một khi thông tin của khách hàng bị lộ, họ sẽ trở nên lo lắng về mức độ bảo mật và có thể chuyển sang các đối thủ cạnh tranh, dẫn đến mất khách hàng và doanh thu. Các tổ chức, công ty, có thể gặp phải các vấn đề pháp lý liên quan đến vi phạm các quy định bảo mật dữ liệu như GDPR ở châu Âu hoặc CCPA ở California, Mỹ, điều này có thể khiến công ty phải đối mặt với các khoản tiền phạt nặng.

Một ví dụ điển hình là vụ rò rỉ dữ liệu lớn của Equifax vào năm 2017, khi hơn 147 triệu người bị ảnh hưởng. Công ty đã phải chi trả hơn 700 triệu USD cho các chi phí bồi thường, các khoản phạt và các chi phí khắc phục sự cố. Hậu quả này cũng khiến danh tiếng của Equifax bị ảnh hưởng nghiêm trọng và nhiều khách hàng đã quay lưng với công ty. Do đó, việc bảo vệ dữ liệu không chỉ là trách nhiệm của các tổ chức mà còn là một phần của chiến lược kinh doanh dài hạn để duy trì sự ổn định và phát triển bền vững.

3. Giải pháp tăng cường bảo mật dữ liệu trong kế toán thông qua ứng dụng công nghệ số

Bảo mật dữ liệu trong kế toán luôn là một vấn đề quan trọng, đặc biệt trong bối cảnh công nghệ số ngày càng phát triển và việc sử dụng các hệ thống kế toán điện tử ngày càng phổ biến. Các công ty kế toán cần ứng dụng các giải pháp công nghệ số tiên tiến để bảo vệ dữ liệu một cách hiệu quả. Dưới đây là một số giải pháp tăng cường bảo mật dữ liệu trong kế toán thông qua ứng dụng công nghệ số.

Mã hóa là một trong những phương pháp bảo mật quan trọng nhất trong việc bảo vệ dữ liệu kế toán. Mã hóa giúp biến dữ liệu thành một dạng không thể đọc được nếu không có khóa giải mã thích hợp. Việc áp dụng mã hóa vào các hệ thống kế toán giúp đảm bảo rằng ngay cả khi dữ liệu bị đánh cắp, kẻ tấn công cũng không thể truy cập vào nội dung dữ liệu mà không có sự hỗ trợ từ khóa giải mã. Các công ty kế toán có thể sử dụng các thuật toán mã hóa mạnh mẽ như AES (Advanced Encryption Standard) để bảo vệ thông tin nhạy cảm như số tài khoản, mật khẩu và các giao dịch tài chính. Đặc biệt, việc mã hóa dữ liệu trong quá trình truyền tải qua các mạng công cộng sẽ giúp ngăn chặn các cuộc tấn công như nghe lén...

Một giải pháp quan trọng khác để bảo vệ dữ liệu kế toán là sử dụng phần mềm bảo mật và các hệ thống tường lửa (firewall). Phần mềm bảo mật giúp phát hiện và ngăn chặn các phần mềm độc hại, virus có thể xâm nhập vào hệ thống kế toán và làm lộ thông tin tài chính. Tường lửa đóng vai trò là một lớp bảo vệ giúp ngăn chặn các truy cập trái phép từ bên ngoài vào hệ thống kế toán. Các phần mềm bảo mật hiện đại có thể quét toàn bộ dữ liệu và các luồng thông tin vào và ra khỏi hệ thống để đảm bảo rằng không có nguy cơ bảo mật nào bị bỏ sót.

Xác thực đa yếu tố (MFA) là một giải pháp cực kỳ hiệu quả trong việc bảo vệ hệ thống kế toán khỏi các mối đe dọa từ việc xâm nhập trái phép. MFA yêu cầu người dùng phải cung cấp hai hoặc nhiều yếu tố xác thực, chẳng hạn như mật khẩu kết hợp với mã xác nhận từ ứng dụng di động hoặc mã OTP (mã một lần). Việc áp dụng MFA giúp tăng cường độ bảo mật, bởi vì ngay cả khi một kẻ tấn công chiếm được mật khẩu của người dùng, họ

cũng sẽ gặp khó khăn trong việc vượt qua yếu tố xác thực thứ hai. MFA là một giải pháp bảo mật cực kỳ quan trọng trong việc bảo vệ hệ thống kế toán trực tuyến, đặc biệt là khi nhân viên làm việc từ xa hoặc sử dụng các thiết bị di động để truy cập vào dữ liệu.

Điện toán đám mây không chỉ mang lại lợi ích về chi phí và hiệu suất mà còn giúp tăng cường bảo mật dữ liệu kế toán. Các nhà cung cấp dịch vụ đám mây thường có các biện pháp bảo mật rất mạnh mẽ, bao gồm mã hóa dữ liệu, sao lưu dữ liệu tự động và bảo vệ khỏi các cuộc tấn công mạng. Khi sử dụng dịch vụ đám mây, các công ty kế toán có thể giảm thiểu rủi ro mất mát dữ liệu do sự cố phần cứng hoặc các cuộc tấn công mạng. Bên cạnh đó, việc lưu trữ dữ liệu trên đám mây giúp doanh nghiệp dễ dàng truy cập và chia sẻ thông tin từ bất kỳ đâu mà vẫn đảm bảo an toàn.

Ngoài các giải pháp công nghệ, một yếu tố không kém phần quan trọng trong việc bảo mật dữ liệu kế toán là đào tạo và nâng cao nhận thức bảo mật cho nhân viên. Nhiều vụ rò rỉ dữ liệu xảy ra không phải do lỗi hệ thống mà là do nhân viên không tuân thủ các quy tắc bảo mật cơ bản. Do đó, các công ty kế toán cần tổ chức các khóa đào tạo thường xuyên về bảo mật, cung cấp cho nhân viên những kiến thức cần thiết về cách bảo vệ thông tin và nhận biết các mối nguy hiểm từ các cuộc tấn công lừa đảo hoặc phần mềm độc hại. Đồng thời, việc xây dựng một chính sách bảo mật rõ ràng và có hệ thống cũng giúp đảm bảo tất cả các nhân viên trong công ty đều tuân thủ đúng các quy trình bảo mật khi làm việc với dữ liệu kế toán.

Một giải pháp không thể thiếu để bảo vệ dữ liệu kế toán là giám sát và kiểm tra an ninh hệ thống liên tục. Việc theo dõi và phân tích các hoạt động trong hệ thống giúp phát hiện kịp thời các dấu hiệu bất thường, từ đó có thể ngăn chặn hoặc giảm thiểu thiệt hại nếu có sự cố xảy ra. Các công ty kế toán có thể sử dụng các công cụ giám sát tự động để theo dõi lưu lượng mạng, phân tích các hành vi truy cập hệ thống và phát hiện các mối đe dọa tiềm ẩn.

3. Kết luận

Bảo mật dữ liệu trong lĩnh vực kế toán không chỉ là một vấn đề công nghệ mà còn là một chiến

lược quản lý quan trọng. Việc ứng dụng công nghệ số trong việc bảo vệ dữ liệu kế toán giúp doanh nghiệp không chỉ tuân thủ các yêu cầu bảo mật mà còn nâng cao độ tin cậy với khách hàng, đối tác và cơ quan quản lý. Việc áp dụng các giải pháp công

nghệ số như mã hóa dữ liệu, xác thực đa yếu tố, sử dụng phần mềm bảo mật và điện toán đám mây sẽ giúp các công ty kế toán bảo vệ thông tin tài chính và nâng cao khả năng phòng ngừa các mối đe dọa từ tội phạm mạng ■

TÀI LIỆU THAM KHẢO:

Diễn đàn Kinh tế Thế giới (WEF) (2022), Báo cáo Rủi ro toàn cầu 2022.

IBM (2021), Khảo sát An ninh mạng.

Hiệp hội Kế toán Công chứng Anh quốc - ACCA (2020). Nghiên cứu "The Future of Audit and Assurance 2020".

Verizon (2023), Data Breach Investigations Report 2023.

IBM (2023), Cost of a Data Breach Report 2023.

Ngày nhận bài: 9/1/2025

Ngày phản biện đánh giá và sửa chữa: 20/1/2025

Ngày chấp nhận đăng bài: 10/2/2025

ENHANCING DATA SECURITY IN ACCOUNTING THROUGH THE APPLICATION OF DIGITAL TECHNOLOGIES

● **NGUYEN QUANG HUNG**

Faculty of Accounting and Auditing,
University of Economics - Technology for Industries

ABSTRACT:

This study analyzes the major data security risks facing the accounting sector in the digital age and proposes modern technological solutions, including the application of artificial intelligence (AI), blockchain, and automation. The study aims to support businesses in strengthening the protection of financial information against increasingly complex threats. Additionally, the study highlights the necessity of developing a comprehensive security strategy to minimize potential losses and enhance customer trust, thereby contributing to the sustainable growth of enterprises in the digital economy.

Keywords: data security, accounting, AI, blockchain, information security.