yubico

3 steps to strengthen security for privileged users across financial services

At approximately $5.86 million, the average total cost of a data breach for the financial services industry is significantly higher than less regulated industries[1], and Forrester estimates that at least 80% of data breaches have a connection to compromised privileged credentials[2]. Privileged credentials play a crucial role in a hackers ability to compromise critical systems and infrastructure as these offer unrestricted access to confidential and sensitive applications and services, and ultimately financial and strategic data and customer account information. Because of this, privileged users are often the targets of spear phishing. While phishing emails are sent to a broad audience at random with the expectation that a few will respond, spear phishing emails are carefully designed and more personalized, to ensure that the recipient responds or clicks through to a fake website that then captures user credentials. To do this, cybercriminals use social media and other publicly available information to tailor emails toward the intended recipient.

To ensure that privileged accounts don't fall victim to account takeovers, financial services organizations need to ensure strong authentication for privileged users before giving them access to sensitive and confidential applications, services and data.

Below are three steps that financial services organizations can take to strengthen security for privileged users:

1 Identify accounts and services that contain confidential and PII data

The first step in strengthening security for privileged users is to identify high risk accounts and services that contain sensitive and confidential information. This information can be anything from budget plans to strategic documents, core banking systems, HR systems containing payroll information, and customer/transaction databases. Flagging these accounts and services will enable financial services organizations to ensure strong authentication security is implemented. Additionally, with rising public, private and hybrid cloud adoption, it's important to include SaaS and IaaS hosted applications in this exercise.

2 Identify who really is a privileged user

Step two is to identify all privileged users across the company. Many organizations think that a privileged user is someone like a database administrator, systems administrator or network administration–roles that typically have broader access and privileges compared to non IT roles. But these are only a small subset of who a privileged user really is. A privileged user is any user that has access to confidential and sensitive data, including employees within C-suite, HR, finance and accounting, and application development. The identities of these privileged users is the new security perimeter that needs to be protected, as opposed to the network itself.

[1] 2019 Cost of a Data Breach Report, Ponemon Institute

[2] The Forrester Wave™: Privileged Identity Management, Q4 2018 November 14, 2018

3 Strengthen security by deploying strong MFA for privileged users

Passwords are easily breached and aren't strong enough to protect privileged accounts. Privileged accounts can be strengthened by deploying strong multi-factor authentication (MFA) in addition to usernames and passwords. But not all MFA is created equal–mobile-based authentication such as SMS, OTP codes and push notifications don't protect against malware and man-in-the-middle attacks. These also make the company liable for mobile related reimbursement costs. Instead, a hardware security key such as the YubiKey, is the only way to ensure 100% protection against account takeovers[3].

YubiKeys protect privileged users from phishing and account takeovers, enabling secure privileged access management

The Yubikey is a hardware security key that helps ensure all privileged users follow a higher bar of security, in turn protecting financial services organizations from account takeovers. Because the YubiKey is based on hardware and the authentication secret is stored on a separate secure chip built into the YubiKey, it cannot be copied or stolen. This makes it the best security for authentication privileged users. Financial services organizations can quickly get started with strong MFA for privileged users using the YubiKey as they don't require a re-architecture–YubiKeys work with leading Identity and Access Management (IAM) platforms, making it easy to integrate into existing architectures.

[3] Research by Google, NYU, and UCSD based on 350,000 real-world hijacking attempts. Results displayed are for targeted attacks

About Yubico Yubico sets new global standards for easy and secure access to computers, servers, and Internet accounts. Founded in 2007, Yubico is privately held with offices in Australia, Germany, Singapore, Sweden, UK, and USA. Learn why nine of the top 10 internet brands and millions of users in more than 160 countries use our technology at www.yubico.com.

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Sweden

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 USA
844-205-6787 (toll free)
650-285-0088