WHITE PAPER

How PKI Helps Safeguard Your Workforce

Picture this: your organization stays on top of patching its software, keeps devices, network endpoints and 3rd party servers secure, and employs advanced threat detection to fight breach and loss. And then Lisa from HR opens an email from "The IT Department" requesting her credentials for payroll software for a seemingly legitimate reason. She sends those credentials, thinking she's doing the right thing. Millions of dollars later, the hole in your network security strategy is painfully clear: the user.

In Verizon's 2019 Data Breach Investigations Report, the two top actions implicated in breach are phishing and stolen credentials—both of which can be accomplished through relatively low-tech means that revolve around social engineering. Our imaginary Lisa from HR was a victim of phishing, which often plays out as someone posing as an authority or fellow employee attempting to obtain credentials from unwary users in an email. These attacks are incredibly effective and are starting to go by a new name: business email compromise (BEC).

The Growing Threat of BEC

BEC is a major threat vector today, and scams have gotten much more sophisticated since the days of the Nigerian prince—especially when it comes to spoofing emails from internal departments, trusted service providers (like Google or Microsoft), vendors, or even CEOs. A "scam alert" PSA issued by the FBI in September of 2019 has this to say about BEC:

> **"[IT] CONTINUES TO GROW AND EVOLVE, TARGETING SMALL, MEDIUM, AND LARGE BUSINESS AND PERSONAL TRANSACTIONS. BETWEEN MAY 2018 AND JULY 2019, THERE WAS A 100 PERCENT INCREASE IN IDENTIFIED GLOBAL EXPOSED LOSSES."**

With BEC losses doubling year over year, not addressing this issue is not an option. Costs are steep, with the FBI citing total international losses due to BEC of over $26 billion from October 2013 to July 2019.

From nonprofits, to public entities, to enterprise, no one is safe from increasingly convincing phishing attempts. These real-world examples show how insidious the threat of BEC can be:

1 Phishermen Net Nearly $37 Million from a European Toyota Subsidiary

A European subsidiary of Toyota, Toyota Boshoku Corporation, fell prey to a BEC scam in 2019 that resulted in losses in the tens of millions—a figure that would destroy smaller organizations. Like most BEC attacks, technological sophistication isn't responsible for these mega losses. Social engineering is everything. Targeting the financing and accounting departments, this scammer successfully convinced employees to transfer money to foreign bank accounts. While wiring money offshore would be a red flag for smaller companies, it's not a rare event in a large multinational corporation, which is potentially why these employees were not alarmed.

2 A Texas School District Is Fooled by Fake Vendors

At the beginning of 2020, Manor ISD (a school district in central Texas) issued a statement regarding losses of $2.3 million due to a BEC scam. Cybercriminals posed as a known vendor and targeted several individuals within the organization via email asking for payment, leading to three separate transactions being sent to criminal bank accounts. The FBI is currently investigating the crime.

3 Patient Data Is Compromised by BEC in a Washington-Based Health System

In 2019, Wise Health was a victim of a focused BEC attack targeting a large number of employees. Several users gave the crook their login credentials, which resulted in the data of nearly 36,000 patients being compromised. The company believes the criminal was attempting to divert payroll deposits as a primary goal, which was unsuccessful. The breach of patient information is a serious liability in itself, regardless of the financial impact.

BEC isn't the only threat associated with the workforce, however. Employee negligence with their credentials or with sensitive material can also be a source of vulnerability for any organization, a factor which can be mitigated if policies are easy to follow and don't rely entirely on users to work.

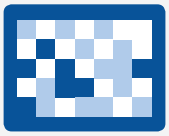
Understanding Digital Certificates for Email Security

A digital certificate for email clients can be used for

SIGNING

and/or

ENCRYPTION



depending on the certificate's attributes.

Two components comprise a digital certificate:

1. A public key (which is used by others to send encrypted email communications to you)
2. A private key (which is used by you to sign emails/documents or unlock encrypted communication)

Public keys facilitate email encryption and can be published or exchanged through a variety of methods:

- Exchanged via a signed email
- Attached to your contact card in your associates email client address book
- Published to a Global Address List (GAL) and shared electronically

Eliminate User Vulnerabilities with Trusted Identities

Certificate-Based Logins for VPN and Windows

What's the safest password? For many enterprises, the answer may be no password at all. With the recent uptick in costly scams, some of which have targeted logon information, finding ways to keep bad actors from compromising credentials or gaining access to network resources can mean simply doing away with traditional credentials for logins in the first place through the use of digital certificates.

One mark in favor of using digital certificates for secure logins is the inherently problematic process of establishing secure password policies, which can be a losing game. Employee-friendly password parameters result in easy-to-crack passwords like "ILOVEYOU123!" while stringent standards may result in sticky-notes with long alphanumeric strings sitting on desks in plain sight—a recipe for credential theft. Your users' minds can only hold so much information before they need to find ways to offload the mental burden.

Digital certificates are a way to mitigate all of these factors. HID IdenTrust® TrustID™ allows organizations to issue secure personal certificates to users that are trusted across operating systems, virtual private networks (VPN), business applications, and browsers for use as a factor in MFA or 2FA. They can also be installed in devices, including tokens or smart cards. This powerful option safeguards user identities and thwarts a breach with the power of PKI.

Secure Emails with Certificate-Based Authentication

Criminals have increasingly started targeting emails thanks to their high degree of user mediation, which can make even a poorly worded spam email dangerous when a gullible or technologically illiterate employee is involved. Compared to DDOS attacks and other kinds of focused hacking, phishing is almost painfully simple. BEC costs businesses millions, so defenses shouldn't just be limited to handbook policies on "not providing sensitive information via email" or other fixes that don't factor in the psychological tricks that cyber criminals leverage in a successful attack. When the CEO seems to be on the other end of the email, is an average employee going to try to implement data integrity rules?

If secure email policies and easy-to-use technologies are in place, however, it becomes a lot harder for criminals to trick employees. IdenTrust® TrustID™ Secure Email (S/MIME) certificates enhance security within your organization's email client. A secure email certificate allows users to determine whether what they've received has been sent by a trusted sender. In a secure email, the content of the message is locked to prevent tampering during transit, preserving its integrity. And with the addition of digital signing, even an intercepted email can't be tampered with or falsified. A Secure Email certificate can also encrypt email messages, which allows the content to be restricted only to authorized viewers.

Spoofing a CEO or payroll manager's identity in a fraudulent email is a much more difficult task when PKI-based security is protecting communication within your company and providing assured identities.

Sign Safely and Easily, Without the Wet-Ink Hassle

From the danger of forgery, to the headaches of storing hard copies, to the challenges presented by remote working, wet ink signing is quickly becoming obsolete. The clerical dimension of dealing with lots of hard copies on an ongoing basis creates opportunities for employee negligence to do damage, as well.

That's where TrustID™ digital certificates come in handy for digital signing and encrypting email. Thanks to the strong encryption functionality and ease of use of digital certificates, digitally signing documents or email becomes simpler and safer resulting in documents and emails that are harder to compromise in transit or stored/at rest. Digital signing with certificates also offers non-repudiation functionality and greater auditability, easing compliance and administrative burden. For regulated industries and government organizations, these features aren't just helpful—they're mission critical.

Finding the Right Trusted Identity Provider

Taking measures to secure user identities, communication, and document signing won't automatically result in reduced risk of breach or loss. It's important to select the right partner to provide a seamless user experience that eliminates gaps in your security strategy.

Here are some questions you can ask when selecting a trusted identity provider:

1. Does the provider offer a "one stop shop" model with the full range of digital certificates to suit my organization's needs?

Remember, the user is almost always the most vulnerable aspect of an organization's security. Dealing with multiple vendors, logins, and overlapping policies because your main partner couldn't provide every digital certificate you need for your enterprise can result in administrative issues. All too often, administrative issues turn into security risks. Select a partner that can fully cover your needs to minimize potential gaps in coverage and user headaches.

2. Is the provider's pricing transparent and predictable?

If you've found a partner whose per-certificate pricing seems incredibly reasonable, you may be thinking that you've found a great deal. That great deal can turn into a nightmare when it comes time for billing if you've used more certificates than anticipated, or if business needs have changed. Consider choosing a partner that can provide you with transparent and predictable pricing that's suited to your organization to make budgeting easier and eliminate costly surprises. In most cases this means choosing a partner that provides a tiered monthly or annual subscription pricing, which eliminates the hassle of managing unexpected billings.

3. Does the provider have a strong trust reputation and use security best practices?

Startups are great...until they aren't. What looks like innovation or market disruption can too often become a source of frustration when functionality isn't as promised, or when their products aren't trusted by existing or legacy resources. When it comes to protecting your workforce, a longstanding reputation of expertise and a top-notch technical pedigree matter. Make sure you find a partner whose mastery of the space and commitment to industry-standard practices are proven in the marketplace.

The IdenTrust Advantage

From industry leaders in the management of trusted identities, HID IdenTrust® TrustID™ certificates deliver versatile security to cover members of your organization and protect against breach and loss. Our certificates are widely trusted and easily integrate with enterprise software and systems, including mainstream browsers, core business applications, and email clients. With transparent, fixed-price options, you can clearly budget for TrustID™ as you protect the enterprise.

IdenTrust® offers options that allow you to do business your way while staying protected, whether you desire self-serve functionality or control across the entire certificate lifecycle. From a turnkey solution through our website that allows members of your organization to download their own certificates, to centralized provisioning accessible via a web browser, to options for integration with smart cards, keys, and other hardware devices, there's a way to make Identrust® TrustID™ certificates work for your unique needs.

About IdenTrust

IdenTrust is a certificate authority providing TLS/SSL certificates, S/MIME certificates, digital signature certificates, code signing certificates, x.509 certificates for user authentication and data encryption, all for one low subscription fee, and no per certificate pricing. IdenTrust certificates are trusted by major operating systems, such as Microsoft, Apple, Google, Mozilla, Adobe and the U.S. Federal Government. For more information about our services visit:

www.hidglobal.com/solutions/identity-access-management/digital-certificates

Individuals can purchase certificates with our certificate selection wizard here. https://www.identrust.com/wizard?nid=185

hidglobal.com

2020-07-29-iams-identrust-workforce-security-wp-en
PLT-04996