cpl.thalesgroup.com

THALES
Building a future we can all trust

ENISA Guidelines for Identity Protection and Phishing Resistant Multi-Factor Authentication

The acceleration of digital transformation for European organizations and the adoption of a hybrid workforce have exposed essential systems and sensitive data to increased cyber threats and risks. The impact and the cost of cyber-attacks are increasing, making the adoption of preventive security measures, such as phishing resistant multi-factor authentication, an existential necessity.

Identity is at the center of modern cyber-attacks

Credential compromise is the most common attack vector – 61% of data breaches are attributed to stolen credentials. Compromised identities facilitate a wide range of attacks, including ransomware. The average cost of a ransomware breach has increased to $4.62 million, while the total cost of a data breach has increased by 10% during 2020 – 2021[1].

ENISA's guidance for multi-factor authentication

The European Union Agency for Cybersecurity (ENISA) has released many guidelines that help national infrastructure industries align their efforts toward meeting compliance with the Network and Information Systems (NIS) Security Directive[2]. The most recent, "Boosting Your Organisation's Cyber Resilience [3]", was published jointly with CERT-EU and provides best practices for all European organizations and agencies to enhance their state of cyber resilience. Most notably, the guidelines include provisions such as:

- Protection of all remotely accessible services with multi-factor authentication. Organizations should avoid using SMS and voice calls as authentication methods. Instead, they should consider "deploying phishing resistant tokens such as smart cards and FIDO2 (Fast IDentity Online) security keys."
- Deployment of multi-factor authentication whenever supported by an application: "These include, but are not limited to, VPN services, external facing corporate portals and email access."
- Ensure users do not re-use passwords and encourage users to use multi-factor authentication (MFA) whenever supported by an application (on social media for instance).
- Control third-party access to corporate networks and systems to prevent inheriting threats and attacks.

1 All statistics, IBM 2021 Cost of Data Breach report, available at https://www.ibm.com/security/data-breach

2 https://www.enisa.europa.eu/topics/nis-directive

3 https://www.enisa.europa.eu/news/enisa-news/joint-publication-boosting-your-organisations-cyber-resilience

- Change all default credentials and disable all protocols that do not support multi-factor authentication.
- Tightly control third party access to internal networks and systems and implement network segmentation and micro-segmentation. This will improve an organization's ability to prevent and detect supply chain and risk of lateral attacks across environments.

Which MFA methods are not phishing-resistant?

Although MFA generally protects against common methods of gaining unauthorized account access, not all multi-factor authentication methods can protect against sophisticated attacks.

Both ENISA and a recent brief by the US National Institute of Science and Technology (NIST) on multi-factor authentication[4] advise against the use of authentication methods that rely on memorized secrets, look-up secrets, out-of-band authentication (SMS/PSTN) including push notification, and one-time-passwords (OTP).

SMS-based OTP

Security experts consider SMS authentication to be vulnerable to SIM swapping attacks and interception over public networks. When an authentication code is sent via SMS to a mobile device, we must be confident that the message reaches the intended recipient. However, research has demonstrated the increasing success of redirecting or intercepting SMS messages without requiring cost or time.

Authentication using Public Switched Telephone Networks

Use of public phone networks is considered insecure due to the risk of device infection or SIM swapping, code interception, authentication spamming and other risks associated with social engineering.

Push OTP

Much attention has focused on OTP Push authentication, which has been widely deployed for its convenience. Although not phishing-resistant, NIST and other security agencies consider it to offer higher security than SMS/PSTN authentication.

Optimizing Secure Access with Appropriate Authentication

ENISA recommends the use of phishing-resistant authentication for its superior security. However, ENISA qualified this recommendation by advising that more secure authentication should be used "where possible". The most widely available phishing resistant methods today are FIDO2 security keys or physical PKI smart cards. Practical considerations relating to hardware management and provisioning, as well as operational constraints, may limit organizations' ability to deploy them for all use cases.

In addition, many organizations have already implemented OTP hardware or OTP Push authentication. For these enterprises, the prospect of ripping and replacing existing implementations can be daunting. Two questions emerge:

- How should organizations balance the need for phishing-resistant authentication with other authentication methods?
- Should they get rid of their OTP authentication implementations?

PUSH OTP, although not phishing-resistant, can be offered as a complementary MFA method for some applications and users, depending on the user profile, the context, and the sensitivity of the data. In addition, when implementing PUSH OTP, or phone-based authenticator apps, there are ways to harden security by:

- Combining PUSH OTP with conditional and contextual authentication. If a login context is considered as high risk, the user could be required to provide additional methods of authentication.
- Combining PUSH OTP with device-native biometrics can demonstrate that an individual intended to authenticate with a specific device.
- Ensuring the integrity of the authentication through risk monitoring, end-point security and anomaly detection.

Ideally, organizations should be able to implement a range of authentication methods, including phishing resistant FIDO2 devices or smart cards. A single type of authentication will not be able to address IT complexity and diverse user populations. For example:

- Not all applications can support FIDO authentication. Alternative methods of authentication would be therefore be needed to enable secure access.
- Some environments, such as factory floors or laboratories, are mobile-free. User logging onto systems under these circumstances would need to use an authentication method that does not rely on mobile phones.

Addressing ENISA's guidelines with Thales OneWelcome IAM solutions

Thales OneWelcome provides an end-to-end access management and authentication platform that meets the cyber-security and multi-factor authentication guidelines outlined in the ENISA publication.

With the OneWelcome Identity Platform, organizations and agencies get a centralized risk-based access platform which supports a broad range of strong MFA and risk-based authentication to protect all services, apps and environments whether hosted, on-premises or in the cloud.

4 https://csrc.nist.gov/csrc/media/Presentations/2022/multi-factor-authentication-and-sp-800-63-digital/images-media/Federal_Cybersecurity_and_Privacy_Forum_15Feb2022_NIST_Update_Multi-Factor_Authentication_and_SP800-63_Digital_Identity_%20Guidelines.pdf

The following table maps the ENISA guidelines with the OneWelcome solution offering.

ENISA Guideline	Thales OneWelcome Solution
Protection of all remotely accessible services with multi-factor authentication	A broad range of authentication options which can support all remote access use cases
Deployment of multi-factor authentication whenever supported by an application	Broad integration capabilities enable support of all applications with diverse protocols, including RADIUS, APIs, SAML, OICD, Agents and app gateways
Ensure users do not re-use passwords	OneWelcome Identity Platform offers a range of passwordless, conditional access, and policy-based enforcement which eliminate the use of passwords.
Control third-party access to corporate networks and systems	A range of authentication methods suited to external uses such as FIDO devices, virtual smart cards or pattern based authentication
Change all default credentials and disable all protocols that do not support multifactor authentication	With policy-based access, the OneWelcome Identity Platform can block access if MFA is not used
Tightly control third party access to internal networks and systems and implement network segmentation and micro-segmentation.	Policy and risk based access can be configured to allow access to pre-defined trust zones and enable organizations to achieve zero trust security.

OneWelcome Identity Platform is an enterprise-wide identity system that supports a broad range of authentication methods, including:

- FIDO2 devices
- Virtual PKI smart card
- PKI smart cards and USB authenticators
- Two factor Push OTP in combination with biometric, contextual and risk based authentication
- Two factor OTP hardware authenticators
- Contextual / adaptive authentication
- Risk-based authentication

Conclusion

The ENISA publication reflects the growing emphasis on access security and multi-factor authentication as foundational to reducing the threat of data breaches and malicious access to sensitive resources.

The guidelines calling for organizations to achieve zero trust security by deploying phishing resistant multi-factor authentication mechanisms can be met by the OneWelcome Identity Platform, which offers integrated access management, and a broad range of multi-factor, adaptive and contextual identity validation methods.

To learn more about how OneWelcome access management and MFA solutions, go to our dedicated website.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

> cpl.thalesgroup.com <

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us