July 21, 2024

Yosi Shavit MBA, CISO, CISM, CDPSE , CC– Information Security & ICS Cyber Expert

Risks of remote connection to an OT network via web applications and ways to mitigate the risk

Introduction

During numerous visits to hazardous materials plants, it has become evident that many plants use web applications, some of which are free, to facilitate remote connections for employees, suppliers, and others. The use of these applications entails numerous threats and risks to the plant, such as MITM (Man-In-The-Middle) attacks, data theft attacks, uncontrolled takeovers by legitimate and illegitimate entities, and more.

Objective

The objective of this document is to minimize, as much as possible, the risk associated with the use of these applications.

Proper Remote Connection to the Organization

It is recommended to allow remote access to the organization using the following practice as much as possible:

- Connect to the organization's GATEWAY (e.g., organizational firewall).

- Authenticate against a managed user identification system (e.g., Active Directory).
- Use unique identification via a 2FA mechanism.
- Break the session as much as possible on its way from the GATEWAY into the organization.
- Connect to a bridging server first (e.g., terminal server).
- Maximize the hardening of the server that provides initial access.
- Minimize permissions for the server that provides initial access.
- Perform a compliance check of the remote connecting computer (at minimum, check for up-to-date operating system and up-to-date antivirus).

Secure remote connection to the organization using a web application

f organizational constraints prevent connecting as outlined in Section 3 of this document and web applications are still used, the following compensatory controls should be implemented to minimize risk:

1. Use only purchased software and avoid downloading free versions from the internet (especially when licenses expire or for any other reason) as they may be compromised.

2. Block the download of free versions using organizational content filtering.

3. Regularly update the software, particularly with security updates.

4. Create and manage either White Lists or Black Lists as decided by the organization, with a preference for maintaining a White List that specifies authorized users.

5. Monthly review and prune the White List, removing any unidentified or unauthorized users.

6. Use strong passwords with at least 8 characters and complexity of at least 3 out of 4 categories (uppercase letters, lowercase letters, numbers, special characters).

7. Implement Two-Factor Authentication (2FA) in the product.

8. Disable the quick access feature in Team Viewer that allows connections without requiring a password.
9. Do not install the product on critical and sensitive servers, such as AD, DBA, or any other critical organizational server or any component related to the automated control system.
10. Use encrypted VPN communication to prevent data or credential theft.

Yosi Shavit CISO, MBA, CISM, CDPSE
Head of ICS Cyber Security Department
Ministry of Environmental Protection
Phone 972- 74-7675850| Cellular 972-58-6662242
yosish@sviva.gov.il | yosish@indu-sec.co.il | yosish@gmail.com
http:// www.indu-sec.co.il

Yosi Shavit MBA, CISO, CISM, CDPSE , CC– Information Security & ICS Cyber Expert