Covid-19 (Coronavirus) IT Security Considerations

Coronavirus phishing scams

Cyber criminals already try to benefit from the recent developments (Covid19) and are sending fake security updates, IT alerts and software notices that attempt to obtain user credentials or install malware. It is important to keep on top of new vulnerabilities and scams by subscribing to various threat-sharing groups. We also recommend to consider:

1. Implementing coronavirus-specific phishing training or testing;
2. Redistribution of any company policies that cover the use of personal computers, smartphones, tablets and WiFi networks for work and emphasize that:

   (a) those policies still apply to those working from home, and

   (b) security protocols will not be relaxed absent a clear change in policy.

3. Avoid sending legitimate emails to employees that look like phishing emails, so official COVID-19 updates to employees should have a consistent format and not include links or attachments, which will help employees properly identify phishing emails.

Home Office / Remote Capacity / Ressources for the Help Desk

Consider testing the company's remote capacity by having many employees try to login remotely simultaneously, and consider adding or expanding use of secure, web-based video conferencing options which protect your privacy and are GDPR compliant.

Anticipate the additional burden on the IT help desk and make sure those employees have the policies, training and tools they need to handle the increased number of requests for technical assistance from people working from home, including the ability to verify the identity of employees using measures like phone number authentication, challenge questions and two-factor authentication. Employees who experience difficulties using their home computers (for example, printing) will be tempted to use less secure means to accomplish work tasks, such as emailing confidential documents to their personal email accounts so that they can be easily printed at home. Companies should try to anticipate and solve for these problems ahead of time.

Essential Employees / IT Infrastructure

Ensure that contact information is up to date for key employees, especially mobile numbers.

Determine how many people, if any, will be needed on-site to protect the network, including patching systems and conducting information security reviews of any new systems that need to be added in haste throughout this period, as well as those needed to conduct investigations and remediation if a cyber event were to occur.

Consider backup personnel in case some of those people become unavailable.

Coordinate with the company's key third-party data vendors to make sure that their cybersecurity contingency plans are adequate.

NÄGELE Attorneys at Law LLC
Dr. Grass-Strasse 12 | FL-9490 Vaduz | Principality of Liechtenstein
T. +423 237 60 70 | office@naegele.law | www.naegele.law