BlueVoyant

COVID-19 CYBER ADVISORY

The COVID-19 outbreak has been classified as a global pandemic by the World Health Organization. Responding to the pandemic is presenting a challenge for companies as they close their physical offices completely or mandate remote work for their employees. While these measures are an absolute necessity to maintain the health of employees and the continuity of business, they also introduce new and different cyber threats to the organization.

Threat actors have already taken advantage of the situation and despite their claims to the contrary, we expect to see their activity and efforts increase. We anticipate a broadening of the attack surface, exploitation of remote connectivity, and manipulation of employee fears and vulnerabilities as new social engineering attacks are deployed.

Further complicating the situation are IT teams working remotely and "making things work" to keep business and productivity on target in a swiftly changing situation. In addition to the challenges of a sudden move to remote work and a potentially significant increase in the number of external endpoints, employee behaviors are also changing, which increases demands on security teams and SOCs to determine genuine threats.

What can you do to take a proactive approach in this changing landscape to reduce risk?

Educate Your Employees

- About new attacks and fraud attempts that may be used to motivate their fear into action
- About how to identify phishing attempts and social engineering attacks
- About basic protections, particularly on personal devices used for remote work
- About the difference between home and public networks
- About applying strong Wi-Fi password usage for home networks

Update Your VPN

- Ensure proper VPN configuration
- Change passwords and ensure strong password practices are in place
- Use multi-factor authentication
- Grant access on a need-to-have basis

Protect Your Endpoints

- Enable firewalls
- Deploy cybersecurity endpoint protection like next-gen anti-virus and EDR
- Deny inbound communications from untrusted, external devices
- Restrict access to internal applications from personal devices
- Discourage or prohibit the use of free and public network for Wi-Fi access

There are many additional safety measures you can implement, but basic protections are a good start. Considering your resources are stretched with the sudden implementation of remote work, your identification and response to a breach may be delayed. We recommend you also review your Incident Response Plan, and if not already implemented, your Business Continuity Plan and Disaster Recovery Plan.

DISCOVER THE BLUEVOYANT DIFFERENCE | WWW.BLUEVOYANT.COM | CONTACT@BLUEVOYANT.COM