CORONAVIRUS (COVID19) 5 STEPS TO PREVENT CYBERSECURITY THREATS RELATED TO REMOTE WORKERS

The coronavirus (Covid19) has created new challenges for companies seeking to continue their operations while most of its employees work remotely. Offering remote access to your workers requires careful planning and implementation to avoid creating security breaches.

Adjusting to this rapid & urgent change within the company's structure can sometimes result in overlooking critical steps to protect your network. Criminals are aware of the sudden surge of remote workers and are focused on exploiting any weaknesses.

Offering remote access can expose your operations to risk. Your environment can easily be infiltrated, operations interrupted, your company's data and that of your customers exposed to leaks.

TOP 5 Actions To Safely Manage Remote Workers:

1. Take the time to complete your design before implementing an incomplete solution that could create security breaches and put your operations, your data and that of your customers at risk.

Elaborate a detail design based on assets and data classification. Consider user rights based on profiles and groups. Control applications and network segments by user groups considering the lowest right required and reject every access that doesn't meet these requirements. These design rules required minimum security controls already in place. Never allow global access to all users and reject every access that doesn't respect your design rules.

2. Configure your solution step-by-step based on your design to offer safe use of your environment while avoiding omitting certain essential measures. Don't use a trial-and-error approach that will create breaches that you will not be aware. Apply security recommendations and patches available, remove default and test configurations.

3. Perform the required tests (no global access, access by user groups and rights, access control to every asset, applications and networks, monitoring, log entries, alerts generation, etc.) and isolation of every VPN channel to ensure that your solution works according to every specifications and that the security measures are adequate.

4. Closely monitor the security perimeter and user rights so as not to allow unauthorized access or to confidential data.

5. Monitor access to the environment and data by user groups so as not to be the victim of data leaks.

These actions should be completed with a VPN configuration document for every type of user; package setup the user installation to reduce error and offer user support.

These essential rules will complement the security setup and measures already in place, which are essential to control access to your technological environment.

SecurEcom Advisory Services supports organizations in protecting their Data, Applications, Infrastructure, Cyber Security and helping them manage their risk.

During the past 20 years, SecurEcom's team of highly skilled experts in IT, IT & Cyber Security & Risk Management, have supported clients in Quebec, Canada and the United States.

Prominent clients operating in the telecommunications, banking, transportation, insurance, energy, technologies, government and public sectors attracted by SecurEcom's innovative expertise have awarded the company important mandates to redress their IT & Cyber Security and IT Risk management projects.

Please contact us: Alain Scherrer, Principal managing partner:

Alain.Scherrer@securecom.ca, phone: 514 544-0442, extension 2320

Securecom.ca

Indik-dashboard.com