Avast Business

Cybercrime

The New Downtime Threat to SMBs

A growing number of small to medium-sized businesses are falling victim to cybercrime. However, not all SMBs are aware of the risks and implications.

Cybercrime is a massive market.

Worldwide revenues from cybercrime are estimated at $1.5tn annually. Here are just a few of the earnings:

$1bn from ransomware

$860bn from illicit/illegal online markets

$160bn from data trading

$500bn from intellectual property theft

$1.6bn from crimeware-as-a-service

Cybercrime cost businesses a collective $2.7 billion in 2018

The impact of cyberattacks on SMBs

Just one attack can cause data loss, downtime, or other damage that can disable an entire business.

3 in 5 SMBs have experienced a cyberattack in the last 12 months

40% of infections spread to multiple devices throughout the network

20% of those businesses attacked had to cease operations immediately

$34,604 average cost to SMBs for cybercrime in the last 12 months

8hrs - 1wk The amount of time businesses spent wiping and restoring all the infected computers

SMBs need a strong security defense

Proactive security should include services that protect data, devices, and people to eliminate gaps in protection.

Devices	Data	People
Antivirus Installing and monitoring antivirus on all devices – from PCs to mobile phones – is the best protection around.	**Secure web gateway** A cloud-based secure web gateway protects your network from web-based threats by preventing users – even roaming ones – from inadvertently downloading malware or accessing phishing sites.	**Secure authentication** There are many ways to achieve this but defining password policies and using SSO and MFA are good first steps for an SMB.
Patch management All software systems come with vulnerabilities, but they can be resolved by installing patches and keeping software up to date.	**Email encryption** End-to-end email encryption ensures only the sender and receiver with a decryption key can view the contents of the email and any attachments.	**Secure remote working** Remote workers need a VPN connection to their company network that encrypts all traffic to provide them with secure access to company data and applications.
Regular vulnerability scans Vulnerability scans should be done regularly and include the status of antivirus software, password policies, and software updates.	**Data loss prevention** A DLP solution prevents end users from sharing sensitive data outside the company network by regulating what data they can transfer.	**Security policies** Define security policies, which include what data needs to be protected and how, and make this information available so everyone understands their role in keeping the business safe.
Web server hardening Web servers usually sit at the edge of a network making them more vulnerable to attacks. Proper hardening ensures default configurations are changed and that certain services and displays are disabled.	**Backup and recovery** Even though you have taken every precaution, it is important to have a solid backup solution in place so you can restore operations quickly.	**Security awareness and training** People cannot defend themselves against threats they are unaware, so it is crucial to educate employees on ways to protect themselves.

Don’t let your business become a cybercrime statistic.

Contact us to learn more about protecting your business.

Sources:
http://bit.ly/2jLZq9a
http://bit.ly/2y4svWK
http://cnnmon.ie/2tGFWGv
http://cnet.co/2tYilvY
http://cnet.co/2f7hBYa