kindred

Security Newsletter

2 November 2020

Subscribe to this newsletter

Enterprises confident Chief Sustainability Officer (CSO) will improve cybersecurity

As the move to quell the spreading coronavirus, business made a quick switch--an office overhaul--and sent its workforce to do their duties remotely, which presented an entirely new series of security challenges. Nearly all (98%) enterprises believe cybersecurity will improve a sustainable development strategy and the specific role of a Chief Sustainability Officer (CSO), according to new research from Kaspersky's latest, "The State of Industrial Cybersecurity in the Era of Digitalization."

Because of the unprecedented track of businesses during the COVID-19 pandemic, industrial companies were forced to prioritize cybersecurity. In 2019, 40% of large enterprises planned to report on cybersecurity risks to boards of directors annually, but this year, according to a Gartner report, 100% will do so.

Major challenges found are "damage of service quality, "loss of confidential information" and "mitigation costs." The last major challenge, "mitigation costs," was less of a critical issue in previous years, and it now requires special and occasionally expensive resources. Respondents (24%) found internal security practices need to be revisited during the pandemic, but only 15% suggested employees need special security training, as they work from home during the pandemic. The report recommends better preparation for lockdown working conditions, access of corporate networks limited to the use of company-owned devices only.

Read More on TechRepublic

Kaspersky Report

FBI, DHS, HHS Warn of Imminent, Credible Ransomware Threat Against U.S. Hospitals

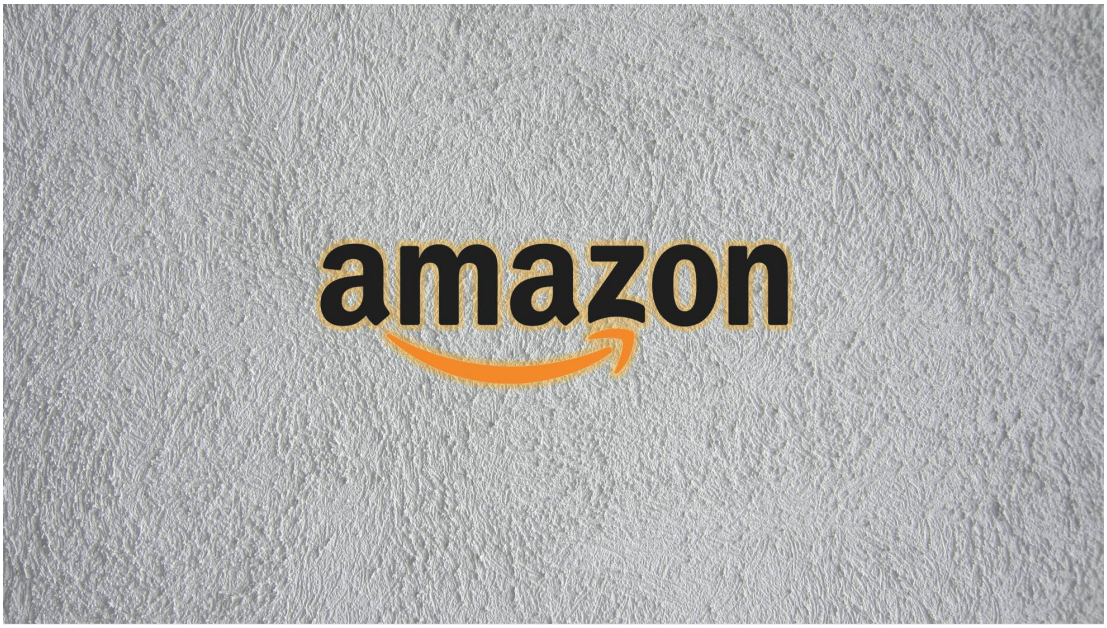
On Monday, Oct. 26, KrebsOnSecurity began following up on a tip from a reliable source that an aggressive Russian cybercriminal gang known for deploying ransomware was preparing to disrupt information technology systems at hundreds of hospitals, clinics and medical care facilities across the United States. Today, officials from the FBI and the U.S. Department of Homeland Security hastily assembled a conference call with healthcare industry executives warning about an “imminent cybercrime threat to U.S. hospitals and healthcare providers.”

The agencies said they were sharing the information “to provide warning to healthcare providers to ensure that they take timely and reasonable precautions to protect their networks from these threats.” One participant on the government conference call today said the agencies offered few concrete details of how healthcare organizations might better protect themselves against this threat actor or purported malware campaign. “They didn’t share any IoCs [indicators of compromise], so it’s just been ‘patch your systems and report anything suspicious’,” said a healthcare industry veteran who sat in on the discussion. However, others on the call said IoCs may be of little help for hospitals that have already been infiltrated by Ryuk. That’s because the malware infrastructure used by the Ryuk gang is often unique to each victim, including everything from the Microsoft Windows executable files that get dropped on the infected hosts to the so-called “command and control” servers used to transmit data between and among compromised systems.

Read More on BleepingComputer

Even More on KrebsOnSecurity

Amazon sacks insiders over data leak, alerts customers



Amazon has recently terminated employees responsible for leaking customer data, including their email addresses, to an unaffiliated third-party in violation of company policies. The company has sent out an email announcement to affected customers following the incident.

"We are writing to let you know that your e-mail address was disclosed by an Amazon employee to a third-party in violation of our policies. As a result, we have fired the employee, referred them to law enforcement, and are supporting law enforcement's criminal prosecution." "No other information related to your account was shared. This is not a result of anything you have done and there is no need for you to take any action. We apologize for this incident."

Although the email notification pins blame for the incident on "an Amazon employee," a company statement shared by Motherboard implies multiple insiders could be to blame. Insider threats, not all of which may be malicious, continue to pose a risk to tech organizations. Just last month, as reported by BleepingComputer, Shopify had suffered from a data breach impacting 200 merchants, because of some company team members going "rogue." August this year, a Russian national tried to recruit a Tesla subsidiary employee in an extortion effort, "to convince him to deploy an unknown malware strain on the company's computer network." The company did not answer how many customers were impacted.

Read More

More #News

- The 10 vulnerabilities most commonly discovered by bug bounty hunters in 2020
- Don't wait for a breach before implementing cybersecurity
- Home Depot blunder emails customer order info to strangers
- Aetna Fined $1 Million After 3 Data Breaches
- Medical Records of 3.5 Million U.S. Patients Can be Accessed and Manipulated by Anyone
- Humans are Bad at URLs and Fonts Don’t Matter
- Microsoft: Disposable emails now available in Exchange Online
- French IT Services Firm Sopra-Steria Confirms Ryuk Ransomware Attack
- FBI: Hackers stole government source code via SonarQube instances
- Finnish psychotherapy clinic discloses data breach, victims extorted
- Massive Nitro data breach impacts Microsoft, Google, Apple, more
- Phishing Campaign Mimics Microsoft Teams Alerts
- Cybersecurity policy is a must in government
- Phishing Scam Costs Wisconsin GOP $2.3 Million

#Patch Time!

- Critical Oracle WebLogic flaw actively targeted in attacks
- SMBGhost - the critical vulnerability many seem to have forgotten to patch

#Tech and #Tools

- Network Pivoting and Tunneling Guide
- On code isolation in Python
- Repo Jacking: Exploiting the Dependency Supply Chain
- GitHub Pages - Multiple RCEs via insecure Kramdown configuration - $25,000 Bounty
- Mapping ATT&CK Data Sources to Security Events via OSSEM
- ThreatPursuit VM: A Threat Intelligence and Hunting Virtual Machine
- Manuka: Modular OSINT HoneyPot for recon techniques
- FIRST: Ethics for Incident Response and Security
- PlumHound - BloodHoundAD Report Engine for Security Teams
- wsb-detect: detects if you are running in Windows Sandbox ("WSB")
- Cheating at Online Video Games and What It Can Teach Us About AppSec (Part 1)

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us