GNTS Technologies
Strategize | Innovate | Deliver

JULY - 17

Industry News

Hewlett Packard Enterprise's Cyber Risk 2016 report, a comprehensive review of the 2015 cybersecurity threat focusing on multiple technologies revealed:

a) Growing malware attack on OS platforms

- **Windows** remains to be the dominant OS platform for attack. Researchers counted between 135 million and 140 million Windows malware samples in 2015
- **Android**, is the 2nd most heavily targeted platform with about 4.5 million malware samples. Over 10,000 threats were discovered daily on the Android platform reaching a total year-over-year increase of 153%
- **Apple's iOS**, remained fairly low in malware targeting, for instance at a mere 70,000 samples. But that number represented a stunning 230% increase from 2014

b) Attackers shifting their efforts to directly attack applications

- Over 35% of the applications scanned exhibited at least one critical or high severity vulnerability
- Mobile applications that suffer from internal system information leaks highlight the concern for storing business critical data on easily lost devices

GNTS offers its expertise in Robotic Process Automation, Artificial Intelligence, Natural Language Processing (NLP), Internet of Things (IoT), Application Development & Maintenance, Cloud Solutions and DevOps.

Research firm IDC predicts about Internet of Things (IoT)

- The number of devices connected to the Internet will reach 30 billion in 2020, up from an estimated 13 billion this year

According to 2016 Global State of Information Security

- Only 36% have a security strategy for IoT
- And in the case of Financial services organizations, employee, customer, and "soft" IP data are the top three targets of cyberattacks, but theft of "hard" intellectual property soared 183% in 2015

According to Forrester

- 53% of information users use their own personal devices for work, install unsupported software
- Over 70% of mobile professionals will conduct their work on personal smart devices by 2018

March 31st is World Backup Day – one day before April fool's day – a chance for us all to avoid a disaster and embarrassment by making sure we have secure backups of all our most important data.

Data, is said to be the most expensive part of a computer; if data is irrecoverably lost then everything is lost.

- 70% of companies that suffer from natural disasters go out of business within a year - and only 6% survive long-term
- Hardware or system failure accounts for 78% of all data loss, while Human error accounts for 11%
- U.S. businesses lose over $12 billion per year because of data loss

And **Downtime** causes:

- Small business to lose around $8,000 per hour
- Medium-sized businesses lose between $74,000 and $90,000 per hour
- And large enterprises rack up costs of between $700,000 and $800,000 per hour

And what about **Disaster Recovery:**

- Only 35% of small businesses have DR plans
- 36% feel their plan is incomplete-only covering back-end infrastructure, essentially protecting the data center, but not desktops or remote offices

According to 'Spiceworks 2016 State of IT report' on IT budgets and tech trends which surveyed 800+ IT pros:

- IT pros don't expect their IT staff to increase in 2016, which means they'll need to keep doing more, with less
- Almost 60% believe their organization is not adequately investing in IT security

ISACA Governance of Cybersecurity 2014 report had revealed that:

- Of all external relations groups, customers receive the least attention when it comes to cybersecurity
- Trained and vigilant employees are essential for detecting those attackers that get through the defenses
- When it comes to cybersecurity, the concept of monitoring extends beyond the use of technology that looks for signs of malware and detects unauthorized intrusions