Actionable Insights into Securing Innovative and Collaborative Environments

Chris Johnson
President & Chief Executive Officer

Janice Pearson
Vice President, Global Content Protection
Matt Lucas’ impersonation of Boris Johnson
Current state of recovery

Ongoing response

1. Made changes to current infrastructure
2. Adopted remote working technologies or implemented physical workflows
3. Integrating collaboration tools and streaming technologies
### Key trends

In a Deloitte study, “Automation was the top transformation action arising from the COVID-19 crisis. Globally and across all regions, roughly two of three companies expect to pursue automation.”

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Organizations are reducing their real estate footprint</td>
</tr>
<tr>
<td>2</td>
<td>Organizations are redesigning their supply chains</td>
</tr>
<tr>
<td>3</td>
<td>New cloud-based workflows are creating opportunities for scale and efficiency by using automation, machine learning, and integration capabilities</td>
</tr>
<tr>
<td>4</td>
<td>Increase in streaming technologies and SaaS applications</td>
</tr>
<tr>
<td>5</td>
<td>Increased use of digital channels for pre-sale, sale, and post-sale activities</td>
</tr>
</tbody>
</table>
Verizon breach data

- 86% Of data breaches were financially motivated
- 55% Of the breaches were perpetrated by organized criminal groups
- 43% Of breaches involved web applications
- 28% Of breaches involved internal threat actors

Source: 2020 Verizon Data Breach Investigations Report, which analyzed 3,950 breaches in the United States
Regional highlights

LATAM
- DDoS: 62%
- Financially Motivated: 71%
- External: 93%

APAC
- DDoS: 29%
- Financially Motivated: 30%
- External: 63%

EMEA
- DDoS: 29%
- Financially Motivated: 48%
- External: 91%

N America
- DDoS: 31%
- Financially Motivated: 33%
- External: 78%

Source: 2020 Verizon Data Breach Investigations Report
Key challenges

1. Shared responsibility model
2. Lack of talent
3. Cyber attacks
4. Misconfiguration errors
Securing applications
# Existing security vulnerabilities now more relevant

1. Improper VPN Access Configuration on a larger scale
2. Lack of logged VPN access to content by administrators - but now on a larger scale
3. Use of personal computers that are not maintained or monitored by IT
4. Personnel working on content from Wi-Fi networks not protected by a software/hardware firewall
5. Work traffic not segregated from other home devices or IoT solutions
Security recommendations

1. THINK BEYOND THE PERIMETER
   - Network monitoring, proxies, multi-factor authentication, and mobile device management

2. VULNERABILITY MANAGEMENT
   - Continuous monitoring, configuration and patch management, and endpoint protection software

3. LEAST PRIVILEGE
   - Restrict users, accounts, devices, and computing processes and monitor access

4. WEB BROWSER PROTECTION
   - Isolated browser or secure gateway technologies to prevent malware and executables

5. EMAIL PROTECTION
   - Use Password managers, encryption, and egress protection software to prevent breaches

6. SECURITY AWARENESS TRAINING
   - Train users on phishing, malware, and social engineering attacks and how to avoid them
Industry assessment observations

250 Assessments conducted March – October 2020

1. Vendors at widely varying levels of maturity

2. Industry standards and best practices require revision and updating

3. Some industry organizations and studios are producing independent security
More information about our services

info@convergentrisks.com
www.convergentrisks.com

Security Assessments
- Cloud Security
- SaaS Applications
- Service Providers
- Site Security
- TPN

Security Consulting
- Design Reviews
- Cloud Migration
- Pre-Assessments
- Privacy Compliance
- SOC2 Preparation

Vulnerability Assessments
- Cloud Configuration
- Code Reviews
- Infrastructure Pen Tests
- Vulnerability Scanning
- Web App Pen Tests