UNLEASH THE POWER OF LIMITLESS CONNECTIVITY
Security & Privacy

From Bolted-on to Built-in: The Journey of Cybersecurity

Casandra Bowes
Principal Security Architect
Comcast
Introduction

• In the past
  • Security was an afterthought
  • Security was bolted on at the end, if at all
    • Or, addressed after a serious incident

• Then …
  • Governments, corporations and consumers were HACKED
    • Data breaches
    • Malware

• Now
  • Security is a top priority for everyone
    • Built into products and services, not bolted on
    • Always a topic of interest, not just after an incident
Security Goes Mainstream

How hackers helped security take a step forward

• Data breaches were making big headlines.
  • Consumer information was being leaked
    • Corporations
    • Governments
  • Hackers were outsmarting outdated “point solution” security controls
    • Multifaceted polymorphic approach
Common Attacks

- Compromised Credentials
- Ransomware
- Brand Phishing
- Voice Fraud
- Internet Facing Applications
Compromised Credential Attacks

• 61% of Data Breaches are caused by compromised accounts

• Common Methods
  • Credential Stuffing
  • Phishing
  • Brute Force password Attacks

https://www.securelink.com/blog/81-hacking-related-breaches-leverage-compromised-credentials/
Ransomware

2021 Stats

• An attack will happen every 11 seconds
• Estimated cost of $20 million globally
• Common Methods
  • Email containing malware
  • Unpatched Vulnerabilities
  • Exposed ports/services with weak authentication for remote access
Brand Phishing

• “Lower my Cable Bill”
  • Scammers pose as cable employees trick customers into providing account information
  • Exposes customers to additional risk of identity theft
Voice Fraud

- Scammers use an unsuspecting customer’s account to place high volumes of expensive calls
  - Estimated cost to providers of $12 billion in lost revenue
- Common Methods:
  - Compromised credentials
  - Outdated PBX Firmware
Internet Facing Application Attacks

It’s estimated that 90% of internet facing applications have security vulnerabilities

- Common Methods:
  - Attacks on Webservers and Databases
    - Cross-site scripting
    - SQL Injection

https://www.darkreading.com/cloud/it-takes-an-average-38-days-to-patch-a-vulnerability
Turning the Tides

• Rule #1 – Assume you will be breached
  • Strengthen your security posture starting with your most critical and most vulnerable assets (perimeter)
    • Zero Trust
    • Improved Incident Detection and Response
    • Multi-Factor Authentication
    • Ransomware Readiness
    • Shifting Security Left
    • Securing your Customers
    • CyberScore
Zero Trust

• The philosophy of “never trust, always verify”

• Outdated “castle and moat” security models do not meet today’s security needs
  • The network perimeter has disappeared

• Shift from IP based controls to Identity based controls

• Assume every user, device, and application is a threat until verified
Improved Incident Detection/Response

• Threat intelligence programs
  • Advanced data collection/analysis capabilities
    • Next Gen SIEM solutions
    • Advanced Filtering
    • Smart Alerting
  • Tools
    • MITRE ATT&CK Framework
    • Purple Team Events
Multi-Factor Authentication

- Can be something you know, something you have, something you are
  - Password + OTP
  - Device + Facial Recognition
- More than 99% effective in stopping PW related attacks
- Companies and consumers alike have recognized the value
Ransomware Readiness

• Address your known vulnerabilities and keep up to date on patches, especially on parameter assets.
• Disable unused services and processes, specifically RDP and SSH, on externally facing systems. If these services must be exposed, use ACLs and multi-factor authentication.
• Use least privilege access models.
• Reduce the blast radius of attacks with network micro segmentation
• Use advanced security tooling for logging, monitoring, and alerting to bring visibility to what’s happening within your environments
• Back-up your systems regularly and encrypt backups
• Have a response plan ready and practice recovery efforts, especially for critical resources.
Shifting Security Left

- Training
  - Train resources on security best practices according to their role

- Coaching
  - Assist with prioritization of security efforts
  - Focus on progress
  - Assimilate security into team norms

- Automation
  - DevOps to DevSecOps
    - Incorporating security into CI/CD pipelines
    - Automated security scans
    - Dev resources as security champions
CyberScoring

- Combines data from various security tools to create an overall view of cybersecurity
  - Creates visibility across the board
    - Drill down/up to any level of the organization
    - Drill down from a centralized dashboard to source tool data
  - Some platforms exist, but are in the early stages
    - Some companies are buying, others are building their own
  - Provides opportunity to better prioritize security concerns based on company’s risk appetite
Securing Customers

Advanced Security Capabilities

- External Credential spill Monitoring and remediation, build this as basic feature for standard security operations
- Deep and Dark web credential advertisement detection and remediation
- BOT attack prevention at Web, API, and mobile authentication interfaces
- Use IP information for “geo velocity” and to determine “geo location” to reduce credential theft
- Implement 2FA or MFA support for consumers and disable less secure authentication methods
- Detection capabilities for credential sharing and compromised accounts
- Work with law enforcement and other enforcement bodies to identify and disrupt the distribution of unlicensed content
Securing Customers

Customer Education

- Partnered with CTAM for streamsafely.com
- Educates customers on safe streaming practices
  - Risks of password sharing
  - Risks of viewing pirated content
Securing Customers

Combating Email Fraud

• Partnered with big tech to secure third party email clients
  • Microsoft
  • Google
  • Apple
• Disable unused 3rd party email clients
• Modernize authentication for 3rd party email clients using oauth
• Implement Email platform anti-abuse capabilities (anti-spam, anti-malware, anti-phishing, anti-viral)
Conclusion

• Security is now in the spotlight!
  • Thanks, Hackers!
• Security is no longer bolted on
  • Security is built into products and services
• Everybody is part of the conversation
  • Companies
  • Governments
  • Consumers
• Let’s keep security part of the conversation!
Thank You!

Casandra Bowes and Harwant Mahal

Principal Security Architect
Comcast
Casandra_bowes@comcast.com
Image Sources

- **Hacker Image** - "Hacker" by Infosec Images is licensed with CC BY 2.0. To view a copy of this license, visit [https://creativecommons.org/licenses/by/2.0/](https://creativecommons.org/licenses/by/2.0/)
- **Attack Image** - "Week 36 - Cyber attack" by Florian F. (Flowtography) is licensed with CC BY-NC-ND 2.0. To view a copy of this license, visit [https://creativecommons.org/licenses/by-nc-nd/2.0/](https://creativecommons.org/licenses/by-nc-nd/2.0/)
- **Data Breach** - "KIB - World's Biggest Data Breaches" by mkandlez is licensed with CC BY-NC 2.0. To view a copy of this license, visit [https://creativecommons.org/licenses/by-nc/2.0/](https://creativecommons.org/licenses/by-nc/2.0/)
- **Access Denied Image** - "Cyber Security - Hacker" by perspec_photo88 is licensed with CC BY-SA 2.0. To view a copy of this license, visit [https://creativecommons.org/licenses/by-sa/2.0/](https://creativecommons.org/licenses/by-sa/2.0/)
- **The Law** - "The Law" by smlp.co.uk is licensed with CC BY 2.0. To view a copy of this license, visit [https://creativecommons.org/licenses/by/2.0/](https://creativecommons.org/licenses/by/2.0/)
Image Sources

- Article Image - https://streamsaferly.com/
- Email Image - "Email customized icon" by ideagirlmedia is licensed with CC BY-ND 2.0. To view a copy of this license, visit https://creativecommons.org/licenses/by-nd/2.0/
- Brand Phishing Image - https://www.flickr.com/photos/182229932@N07/48413930916
- Telephone Image - "1964 Bell Telephone System Advertisement National Geographic August 1964" by SenseiAlan is licensed with CC BY 2.0. To view a copy of this license, visit https://creativecommons.org/licenses/by/2.0/