CLOUDSEC2019

PICTURE THIS!

SEE. SECURE. GO FURTHER.

CLOUDSEC2019

PICTURE THIS!

SEE. SECURE. GO FURTHER.

Access, Authorization & Trust?

Mary Ellen Condon former Security Chair of IDecosystem

Why & How did we get here

- WHY:
  - Information Technology evolution from the 1960s into a ubiquitous presence in almost everything we do.
- History & How:
  - Keys were the equivalent of what has became passwords
    - About 1960 an MIT graduate –thought it would be useful to researchers using this new tool

Journey from 1960 -1970s

- The evolution of Business programs- systems moved slowly
  - The systems were what today we call "custom"
  - Programmers – Analysts were only constrained by the limitations of the compliers
  - Systems were run internally in a room- access to them was physically controlled
- Companies leading the "revolution" IBM, Sperry Rand, UNIVAC, Honeywell

1980s computer security emerges

- IT systems evolved from back office applications, finance, HR etc.
- Use of IT to deliver core business programs/functions gained a solid footing
  - Purchasing
  - Design/engineering - CAD/CAM
  - Billing- Payments
  - Case Management

1990s

- The US's National Institute of Standards & Technology (NIST) issues the first Special Publications for Information Technology Security- computer security
- Connectivity to the Internet enhances opportunities to collaborate begins to raise concerns about security
- Organizations commence penetration testing to identify "any" vulnerabilities
  - Passwords – are not credible, are not taken seriously by "users"

Late 90s– 2000s

- Blackberry phone emerges as a tool-mobile computing is on the cusp
- Of being a plus and a minus–
  - Enhances productivity,
  - Vulnerabilities become more apparent- cyber security gains in importance
    - Public Key Infrastructure (PKI)
    - Common Access Cards (CAC)

Authorization

- You may be known but do you need to access “x”
  - Independent of whatever security clearance the person holds
- Role Based Access
- Segmentation - access limited to a “defined” area vs free access once on the network
- Increased network monitoring
- Cross organizational – Public Key Infrastructure/ Common Access Cards

Zero Trust -why

- Traditional network design/architecture are no longer effective
- Physical boundaries of an organization's network are going/gone
  - It is fast becoming a virtual environment
  - Organizations must collaborate outside the organization
  - No one should be trusted (internal or external)
  - Third party trust is key – reliance on public key/digital certificates

Zero Trust

- 2010 John Kindervag a principal analyst at Forrester Research Inc. created zero trust
- Draws on multifactor authorization (MFA), IAM, analytics, encryption etc.

  It draws upon existing capabilities;

  It shifts access controls to the device or individual or both
- Increased assurance that it is the right person/device for the right purpose

Zero Trust

- It is a rules based solution which requires processes and adherence to them
- Will the "cost" of a strict solution create unintended issues?

  For the organization?

  For the individual?
- In some ways not so different from the audit logs that were used to rebuild a database

Is Zero Trust the end of the line?

- We get smarter about what works, technology evolves and we learn
- The challenge individual control over their information, with whom they share it and for what purpose
  - Idecosystem group set out to address this concept
    - Incremental progress key to gaining support
    - 1st Step creating the Identity Ecosystem Framework (IDEF)

What do you think

- Let’s assume that most organizations move to zero trust
  - Who does it help?
  - What challenges does it create
- If so, what will be the next iteration???

Assess, Authorization and Trust is a journey-- goals easy for the consumer, while providing protection and confidence for all parties.

Join us on the journey

Acronyms

- NIST = National Institute of Standards & Technology
- ISO/IEC = International Standards Organization/International Electronical Commission
- GDPR = The General Data Protection Regulation 2016/679 (European Union)
- Kantara =Kantara Initiative Inc., Identity Ecosystem Framework (IDEF)

US Legislation

- Legislation addressing the role of IT in the delivery of government services- as well as commercial service were passed. They on focused on how the US federal government is to perform their responsibilities– many companies use them as a guide post.
  - Paperwork Reduction Act (PRA) of 1995
  - IT Management Reform Act (ITMRA) of 1996
  - Federal Information Security Management Act (FISMA) of 2002 & modified in 2014

Resources - 1

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

- ISO/IEC's 27000 series is the Information Technology Security Techniques-Information Security Management series
  - https://www.iso.org/isoiec-27001-information-security.html
- NIST SP 800 Series –the first is focused on controls, the second on the risk management framework
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

Resources - 2

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

- GDPR
  - https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

- Kantara- trust marks
  - https://kantarainitiative.org/trustoperations/classes-of-approval/


CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.
THANK YOU
Mary Ellen Condon, Former Security Chair, IDecosystem
www.cloudsec.com
#cloudsec