Watermelons

GREAT SUMMERTIME SNACK, NOT SO GOOD AS AN INFOSEC STRATEGY

“Trusted Zones” – Don’t Believe It

- Many IT organizations have traditionally focused too much on outside threats to the dismay of their CISOs
  - Perimeter Defense
  - Firewalls
  - IDS/IPS
  - Trusted zones – “we don’t need encryption there…”

- Overlooking many key security strategies such as:
  - Defense in Depth
  - Implementing Critical Security Controls
  - Segmentation
  - Encryption
  - Data Classification
  - Awareness and Training

Sadly many organizations are still taking this “Watermelon” approach to Information Security.

The Impenetrable Shell Mentality

- Securing just the perimeter never was adequate
  - Defense in Depth – we have been calling for this forever
  - But even our Defense in Depth strategies have needed to change to combat the types threats we have seen here today

- Todays biggest threats are not trying to pick the lock on our front doors

- They have the keys and are dressed up as one our employees!

We Can Be Our Own Worst Enemy

- 63% of all breaches in 2015 exploited legitimate credentials
  - Verizon DBIR 2016
- Security Awareness Training is too often ineffective
  - Demonstrated by response rates when we do phishing expeditions
- Many of the controls we have relied on focus on preventing threats from outside
  - Too few focus on the insider threat
  - Or the use of valid credentials to perpetrate attacks
- Firewalls, IPS, antivirus, WAFs, secure coding standards, access controls, even periodic account reviews don't do any good if your DBA's account is compromised….

How Do We Defend Against Ourselves?

- Take the old adage of Defense in Depth further
  - We still need all of the traditional security controls, but take an inside out approach
- Know what data you have and where it is
  - Protect your data at the source
  - Know who has access to your sensitive and critical data
  - Know how your sensitive and critical data can be accessed
- Awareness, awareness, awareness!

Where to Start?

- Implement the critical security controls we all know
  - SANS Top 20
  - NIST
  - ISO
  - COBIT
- Implement SIEM and threat intelligence solutions
- Change default passwords
- Auditing and alerting
  - Establish baseline activity
  - Alert on things outside the norm
  - DBA logging on from unknown IP at off time deserves a second look
  - Alert on critical configuration changes

Focus on the Data

- Don’t give DBAs access to the data
  - Separation of Duties (SOD)
  - Implement DBMS tools like Oracle Database Vault to enforce SOD
  - Consider separating DBA from Security Administrator work
- Encrypt data at rest in the database
  - Ensure proper key management is maintained
  - DON'T STORE KEYS WITH YOUR DATA!
  - Key strength
- Encrypt data in transit at all tiers in the application stack

Focus on the Data

- Ensure your have good configuration management, especially your database servers
  - Know your authorized devices
  - Maintain list of authorized accounts
  - Periodically audit your database server configurations
  - Do you have any public database links in your production database?
- Limit connectivity to your databases
  - Segmentation
  - IP filtering for listeners
  - Limit where application accounts can connect from
  - Tight controls on application account credentials to prevent abuse
  - Utilize Database Proxy solutions for non-application connections

In Conclusion

- Looking at Information Security from the data perspective can help prevent valid credential abuse and subsequent security breaches
- By limiting who can get to you sensitive and critical data and how they can access it we reduce the attack vectors
  - SOD
  - Encryption
  - Segmentation
  - Auditing & Alerting
- But it is no substitute for a robust an comprehensive Information Security Program including effective security awareness

QUESTIONS?