Threat landscape

- The nature of threats is changing:
  - In recent years gone from script kiddies to
    - Organised crime
    - Hacktivists
    - State sponsored
- Types of attack have changed too:
  - Denial of Service
  - Phishing/Spear Phishing
  - Social Engineering
- 2016 Verizon Data Breach Digest
  - Majority of the attackers behind incidents were external actors motivated by financial gain
  - As the time for attackers to compromise a target decreases, so too does the time for companies to discover a security incident

Threat landscape

- 2016 Verizon Data Breach Digest
  - 25% of events were discovered in a matter of "days or less"
  - Unfortunately, that percentage is increasing at a slower rate than proportion of compromises that took "days or less" — attackers are one step ahead
  - Not all vulnerabilities are exploited the same:
    - Some in Adobe and Microsoft flaws were exploited in a matter of days, whereas attackers waited months to exploit bugs in Apple and Mozilla
    - On average, threat actors took about a month to exploit a vulnerability, with half of all first exploitation attempts having occurred within a period of between 10 and 100 days

Threat landscape

- 2016 Verizon Data Breach Digest
  - Web apps accounted for the greatest number of confirmed data breaches
  - Occurred particularly in:
    - Finance
    - Information
    - Entertainment
    - Educational
  - Accounting for nearly 40% of all incidents

Threat landscape

- State of Software Security (SoSS) report
  - 97% of all Java applications scanned used a component with a known vulnerability
  - From late 2015 into 2016 fix rates for application vulnerabilities improving
  - 54% of vulnerabilities fixed
  - Up from 51% for previous year
  - This contrasts with an 80% fix rate in manufacturing, indicating that there is some way to go

The Environment

- The majority of companies are already using hybrid cloud
  - In 2016: 71% of companies surveyed were using hybrid cloud (RightScale State of the Cloud Report 2016)
  - 17% of enterprise with 1000+ VMs were running them on public clouds
  - Hybrid environments tend to add, not reduce complexity, Kevin Brown, CTO, IT Division, Schneider Electric
  - Schneider predicts that data infrastructures will develop toward more **edge computing** sites to accommodate new utilisation models

The Results

- Old methods of protection are found wanting
- Gaps are appearing between infrastructures:
  - on-premises
  - Hybrid cloud
  - Public cloud
- Environments are more complex than ever
- Threat actors are changing in:
  - Motivation
  - Methodologies – data manipulation

Thank you!

paul.hearns@mediateam.ie | www.techcentral.ie | www.techfire.ie