PEOPLE-CENTRIC INSIDER THREAT MANAGEMENT

Michael Silvestri
Sales Director DACH, ITM
Proofpoint
msilvestri@proofpoint.com
+49 163 385 385 5
WHERE DO INSIDER THREATS COME FROM?

“I may have clicked on the phishing link in the email”

“Gave my two-week notice. Need to upload the key files”

“USB always comes to rescue on my flight”

62% of incidents

$307K per incident

15% of incidents

$756K per incident

23% of incidents

$817K per incident
PEOPLE-CENTRIC MEANS SOLVING BUSINESS CHALLENGES

Managing insider threats is more than just a SecOps challenge – it involves HR, Business Managers, Legal and Compliance teams.
PEOPLE-CENTRIC MEANS UNDERSTANDING CONTEXT

Investigating insider threats means knowing the whole story – the who, what, where, why, when of user activity that may put organizations at risk.
PEOPLE-CENTRIC MEANS RESPECTING PRIVACY

Organizations need to take individual privacy as seriously as they do protecting intellectual property. Knowing who is doing what, when, where, why.
TRADITIONAL CYBERSECURITY IS FOCUSED OUTSIDE-IN AND LOGFILE-DRIVEN

FIREWALL

ANTI-VIRUS

SIEM

ACCESS MANAGEMENT

INTRUSION DETECTION
Actual situation

ECB Shuts Site After Subscriber Data Breach

The European Central Bank (ECB) has been forced to shut down one of its websites following a cyber-attack which may have compromised customer data.

The bank said in a brief statement that hackers had compromised its bankers’ integrated

Support@specials.mastercard.de

Mastercard data breach affected Priceless Specials loyalty program

Mastercard disclosed a data breach that impacted customer data from the company’s Priceless Specials loyalty program. The American multinational financial services corporation notified the data breach to the German and Belgian Data Protection Authorities...

August 24, 2019 By Perigig Prugman - Protect In Breaking News - Data Breach

McAfee Sues 3 Former Staffers Now at Rival Tanium

Lawsuit alleges sales representatives stole trade secrets from McAfee before joining Tanium.

McAfee has filed a lawsuit against former members of its sales team who left the company for jobs at competitor Tanium in the past year.

The filing, which was first reported by CyberScoop yesterday, alleges that Jennifer Kinney, Alen Coe, and Percy Tejeda participated in a conspiracy to pilfer McAfee sales secrets and customer strategies in their new positions at Tanium.

Tejeda, former director of finance at McAfee, hired Kinney and Coe to join him at Tanium, according to the suit. McAfee then conducted a forensic analysis of Kinney and Coe’s McAfee computers and discovered they had copied and taken sensitive files from the company before they resigned for their new positions at Tanium.

Read more here.
INSIDER THREATS ON THE RISE

- **Increase in BREACHES**
  - 2014-2015
  - 2016-2017
  - 2018-2019

- **MCKINSEY 2018 STUDY:**
  - 50% of data breaches involve an insider

- **PONEMON 2019 STUDY:**
  - 77 days average time to complete investigation
  - $800k average cost of mitigating insider data breach

- **Companies and Data Affected**
  - **Intel**
    - $1B
    - Nation-state spying
  - **Amazon**
    - 600K accounts
  - **SunTrust Bank**
    - $1.5M
  - **Trend Micro**
    - 600K accounts
  - **Google**
    - 19K files
  - **SunTrust Bank**
    - $1.5M
  - **Nuance**
    - 45K files
  - **Coca Cola**
    - 8K files
  - **Delta**
    - 18K files
  - **DuPont**
    - 18K files
  - **Monsanto**
    - Recruited by nation-state
    - $1B loss
    - 700 layoffs
  - **NSA**
    - No public data
  - **Twitter**
    - 6K
    - Nation-state spying
  - **Phillips 66**
    - $1B
  - **AMSC**
    - $1B loss
    - 700 layoffs
  - **Anthem**
    - 80K files
  - **Boeing**
    - 18K files
  - **DuPont**
    - 18K files
  - **Boeing**
    - 18K files
  - **Allen & Hoshall**
    - $425K
  - **Google**
    - 8K files
  - **AMSC**
    - $1B loss
    - 700 layoffs
  - **Tesla**
    - $1B
  - **Phillips 66**
    - $1B
  - **Tesla**
    - $1B
  - **Monsanto**
    - Recruited by nation-state

- **Corporate Diplomas**
  - **Google**
  - **Amazon**
  - **SunTrust Bank**
  - **Trend Micro**
  - **Intel**
  - **Phillips 66**
  - **AMSC**
  - **Anthem**
  - **Boeing**
  - **Tesla**
  - **NSA**
  - **Twitter**
  - **Monsanto**
  - **Allen & Hoshall**
Citrix hacked: Angreifer erhalten Zugang zu Geschäftsdocumenten

The US-American IT-Unternehmen Citrix is a target of a hacker attack on the company's servers. The cyber-criminals want to gain access to the company's intranet. The stock price of Citrix has risen by 3%. On March 6, 2019, the FBI announced that unauthorized access to the company's intranet had been achieved. In a blog entry, Citrix described how the company had reacted to this unauthorized access.

The Hackathon: How do hackers engage for the good of society

A video of a laptop with a red background.
Emerging Security Category Addressing Critical Gaps

DLP & CASB
Complex and easy to bypass

SIEM / UEBA
Mostly network visibility

PAM / UAM
Limited to IT / privileged users only

ENDPOINT SECURITY
Focused on external threats

Seamless Integration into the existing Infrastructure.
ITS HARD TO UNDERSTAND PEOPLE BY LOOKING AT LOGFILES

Video capture for high risk situations
PEOPLE-CENTRIC INSIDER THREAT MANAGEMENT LOOKS INSIDE-OUT
User Anonymization

An anonymized dashboard provides an overview of risk indicators and assigns a number to each individual, shielding their name, role, and picture, completely anonymizing the person behind the actions.

Goal is being compliant in Germany and supporting the working council in executing regulatory compliance and privacy requirements.
400+ Pre-Configured Insider Threat Use Cases

High risk business users, Privileged users, Contractors & 3rd party vendors

**DATA EXFILTRATION**
- Exfiltration to USB/Removable media
- Exfiltration to cloud storage like DropBox
- Exfiltration via large print jobs
- Exfiltration via webmail clients
- Exfiltration via copy/paste

**PRIVILEGE MISUSE**
- Modifying / deleting rows in a database
- Accessing source code during irregular hours
- Connecting by impersonating privileged / disabled user
- Running unauthorized software on server
- Accessing sensitive data of previous employer

**ACCIDENTAL INSIDERS**
- Storing passwords in clear text
- Downloading from insecure websites
- Using unapproved removable media
- Using unapproved websites
- Accidental misconfiguration of cloud infrastructure

**SECURITY CONTROL BYPASS**
- Tampering with security controls
- Accessing websites associated with criminal organizations
- Downloading unapproved software
- Utilizing VPN or Proxy tools
- Using steganography software
Detecting a Data Exfiltration

FLEXIBLE EDUCATION & PREVENTION OF INSIDER THREATS

Proactive alerts:
Detect unauthorized activity and access, risky accidental actions and unwanted data attempts ahead of costly security incidents

Insider threat expertise:
More than 300 indicators of risk based off CERT Institute and customer research

File activity monitoring:
Track files across their lifecycle, from file creation, import and download to detection of potential data exfiltration
Protect from Data Loss
Protect intellectual property from unauthorized or risky exfiltration vectors.

Accelerate Incident Response
Leverage context to understand the who, what, where, when, why of alerts.

Identify User Risk
Quickly understand context around user activity and data movement for high risk users.

Build an Insider Threat program
Create a formal Insider Threat Program based on insider threat playbooks & security frameworks such as NIST SP-800 53, NISPOM and the experience of 1200+ customers.
1,000+ CUSTOMERS
100+ COUNTRIES
Thank You!

Michael Silvestri
Sales Director DACH, ITM
Proofpoint
msilvestri@proofpoint.com