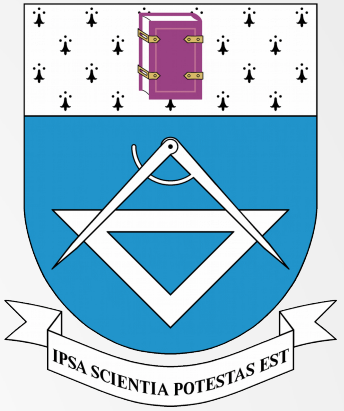


Utilizatorul – ultima linie de aparare în cybersecurity?

dr. ing. Cristian-Mihai Amarandei

cristian.amarandei@tuiasi.ro

Utilizatorul – prima linie de aparare în cybersecurity?

dr. ing. Cristian-Mihai Amarandei

cristian.amarandei@tuiasi.ro

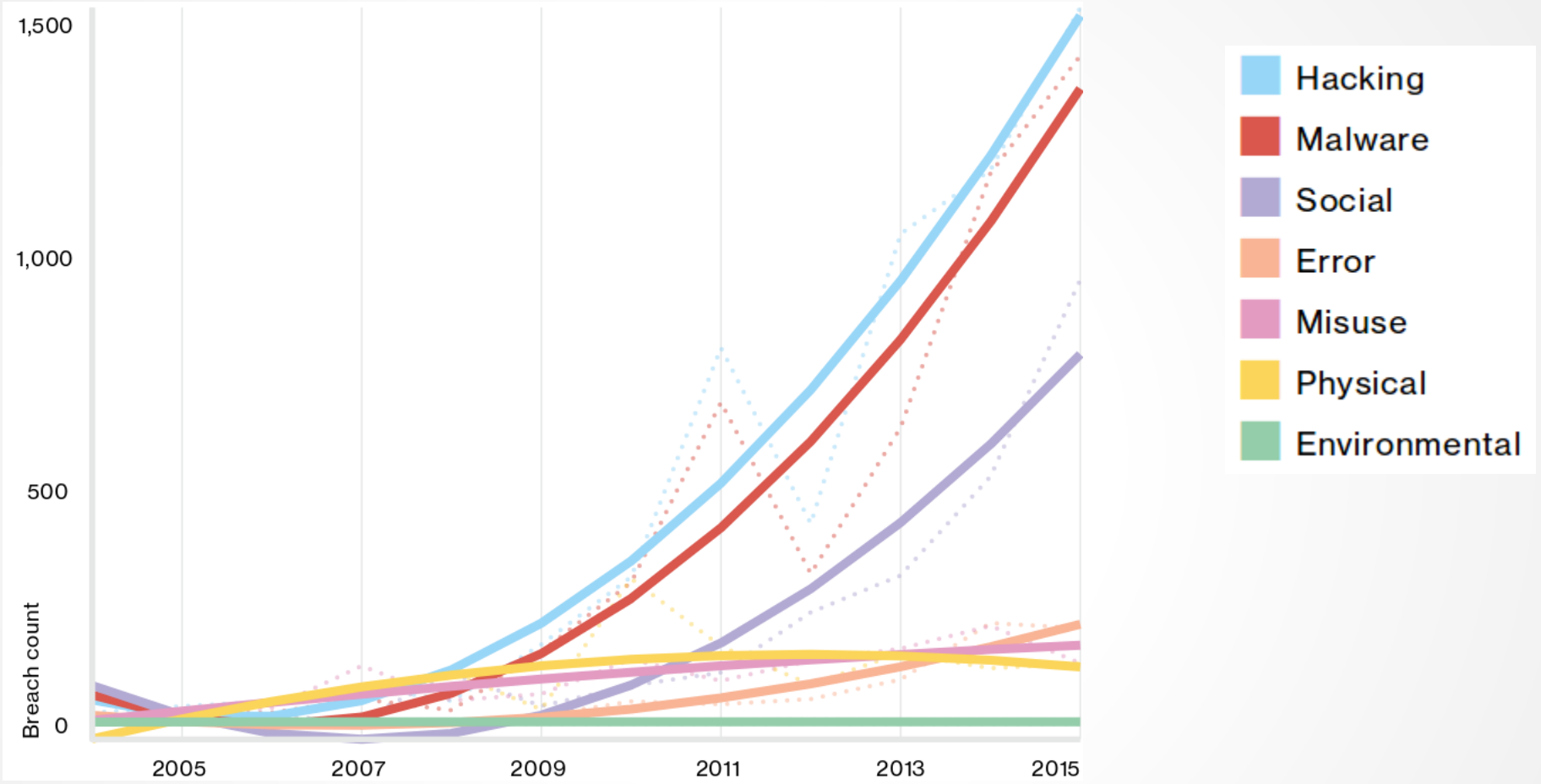
Motivele atacurilor

- Spionaj industrial
- Câștiguri financiare
- Răzbunare (angajat actual/fost nemulțumit)
- …

Amenințări la adresa securității rețelelor

- Hackeri
- Angajați nemulțumiți din diverse motive
- Organizații: sprijinite de guvernele unor țări, organizații teroriste, criminalitate organizată
- Viruși, troieni, malware etc
- Social engineering: - factorul uman
- ...

Verizon 2016 Data Breach Investigations Report



Ce putem securiza?

- Rețeaua
  - Blocarea potențialilor atacatori și mijloacelor de atac cunoscute
  - Securizăm conexiunile cu partenerii de încredere
- Activitățile care necesită conexiune securizată
  - Accesul de la distanță la rețeaua internă
  - Accesul la aplicații și servicii (e-mail, web ...)

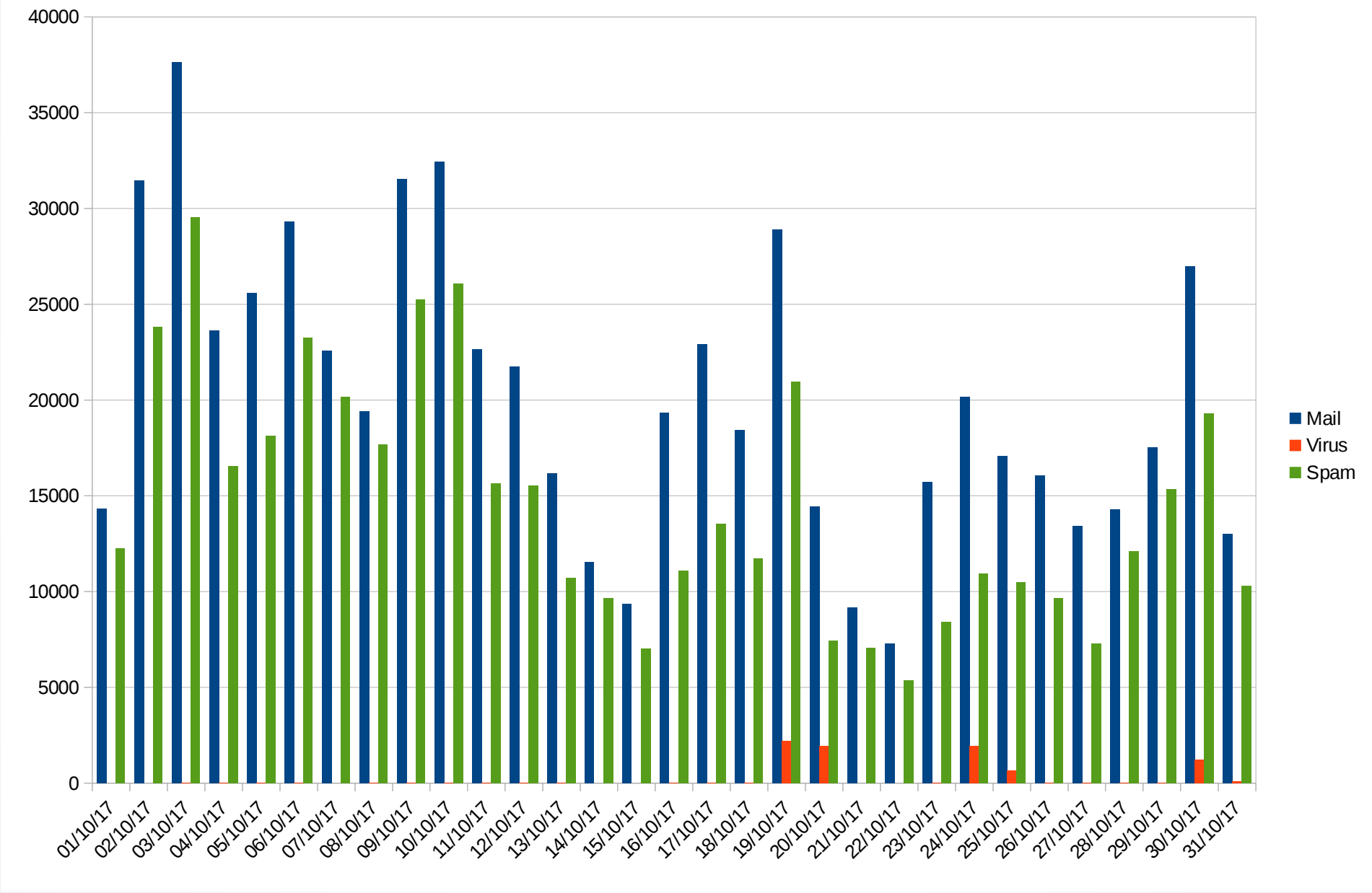
Social Engineering: factorul uman

- Atacatorii pot încerca să obțină acces prin intermediul utilizatorilor
  - Angajații pot fi păcăliți să transmită date de acces la resurse informatice
- **Protejarea utilizatorilor**
  - Organizațiile au nevoie de politici de securitate și de programe de instruire

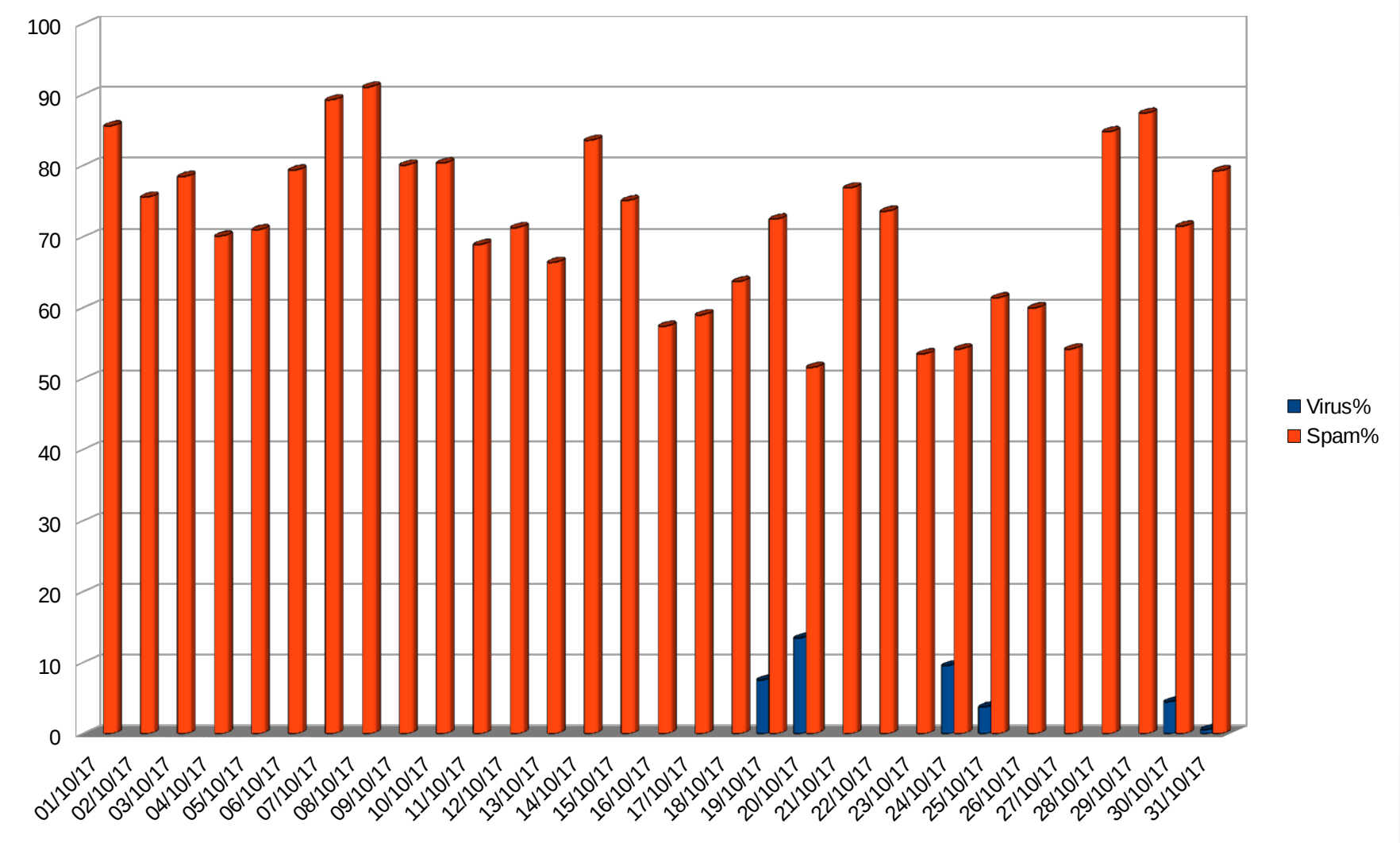
Cum ?

- Politici de securitate/ Regulamente de utilizare
- Achiziție echipamente și de software specializat
- **Educăm utilizatorii !!**

Spam-ul detectat în mesajele de e-mail



Ceva mai multe detalii ….



- Număr total de mesaje email – 624,022
- Spam detectat 452,163 – **72,5%**

după detecția spam-ului și livrarea mesajelor

- Câte din mesajele detectate ca spam conțineau posibili vectori de atac?
- Câte din mesajele care au trecut de sistemul de detecție aveau posibili vectori de atac?
  - De unde și de pe ce dispozitive au fost citite mesajele?
  - Ce a facut utilizatorul?

Politicile de securitate

- Sunt necesare dacă
  - Angajații lucrează cu informații confidențiale
  - Daunele, furtul sau coruperea sistemelor și/sau a datelor pot cauza pierderi financiare importante
  - Organizația are secrete comerciale
  - Angajații au acces regulat la Internet
  - Organizația se supune unor reguli privind securitatea și confidențialitatea informațiilor (**GDPR** !)

Politicile de securitate

- Oferă instrucțiuni angajaților cu privire la modul de gestionare a informațiilor sensibile
- Oferă personalului IT instrucțiuni privind sistemele defensive pe care să le configureze
- Reduce riscul de răspundere legală
- O bună politică de securitate este cuprinzătoare și flexibilă
- Nu este un singur document, ci un grup de documente

Politicile de securitate

- Dacă sunt prea complexe nu le va urma nimeni
- Nu vor avea efect dacă influențează productivitatea
- Trebuie să prezite clar activitățile permise și activitățile interzise în rețeaua și/sau pe echipamentele organizației
- Trebuie să includă clauze generale
- Angajații/utilizatorii trebuie să știe de ce este importantă politica de securitate
  - și consecințele încălcării acesteia!!

Politicile de securitate

- **trebuie implicați reprentanți ai tuturor departamentelor**
- au nevoie de **suport de la cel mai înalt nivel de management**
- utilizatorii/angajații trebuie să semneze documente prin care iau la cunoștință și sunt de acord cu prevederile
- să țină pasul cu tehnologia și cu legile aplicabile

Cum știm dacă politicile sunt bine făcute?

- Standarde internaționale și ghiduri disponibile
  - ISO/IEC 27002:2013
  - Payment Card Industry Data Security Standard (PCI DSS) - https://www.pcisecuritystandards.org
  - National Institute of Standards and Technology (NIST) Cybersecurity Framework - https://www.nist.gov/cyberframework
  - IASME - https://www.iasme.co.uk/

Cum rămâne cu utilizatorul?

- Toți angajații/utilizatorii trebuie educați cu privire la pericolele de securitate și la politicile de securitate
  - **program de instruire riguros!!**
- Angajații pot să detecteze încălcări ale securității
  - sau pot cauza una (accidental !?)
  - pot observa activități suspecte
- **Impunerea** politicilor de securitate!!!

Utilizatorul – prima sau ultima linie de apărare?