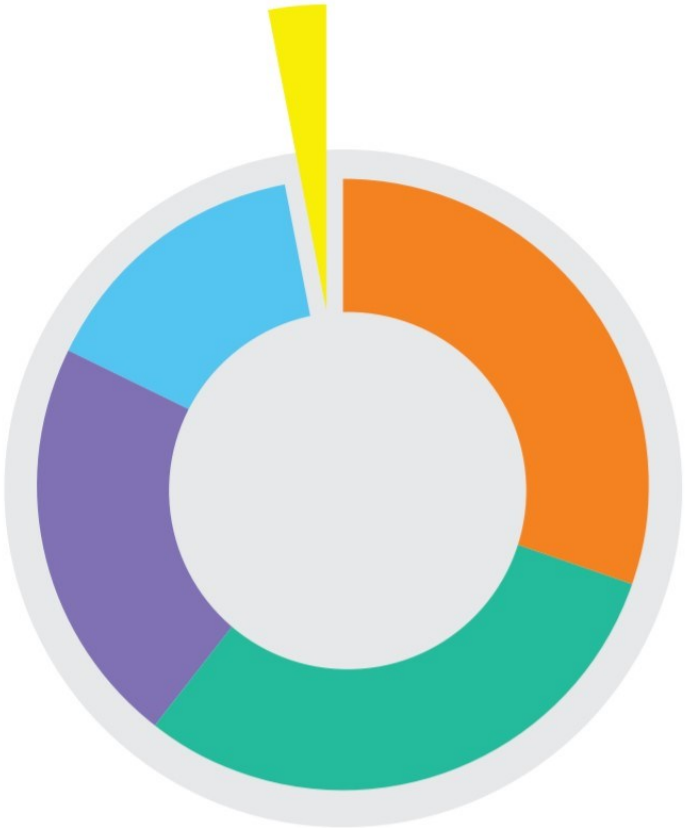
Conștientizarea și mitigarea amenințărilor actuale

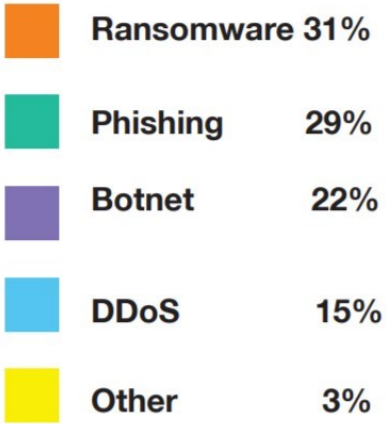
Ioan Constantin
Orange Romania

Provocare

1. Digitalizare rapidă – Digitalizare continuă
2. Suprafețele de atac sunt în creștere
3. Acces rapid și relativ ieftin la malware

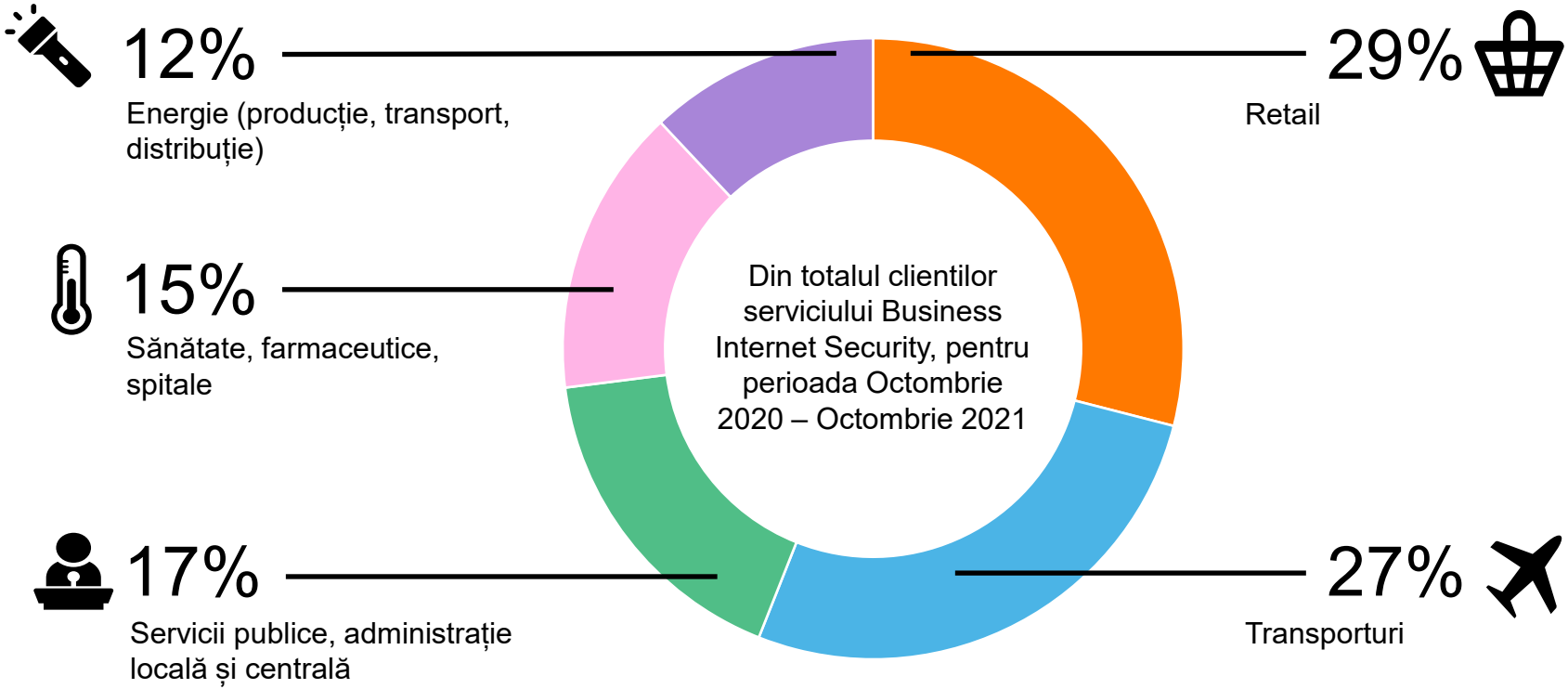
Tendințe





**date din raportul Business Internet Security, Editia a 4-a colectate in perioada Octombrie 2020 – Octombrie 2021*

Distribuția sectorială a atacurilor



Trends 2022

Data Leaks

Pe măsură ce mai multe companii migrează date și servicii în cloud, posibilele breșe de securitate vor aduce compromiterea unor cantități mari de date.

RansomwareaaS

Atacurile Ransomware vor deveni accesibile persoanelor interesate ce vor putea închiria servicii ce permit orchestrarea unor astfel de campanii

Supply Chain

Elemente din lanțurile de producție și distribuție vor fi ținte ale atacatorilor

5G și IoT

Odată cu adoptarea serviciilor și a tehnologiilor 5G în rândul companiilor, acestea vor deveni ținte pentru atactori

Interoperabilitate

Platformele și serviciile IaaS / SaaS vor permite schimbul sigur și rapid de date.

Măsuri esențiale

1

Tehnologie

Asigură un instrumentar tehnologic ce permite crearea unui mediu de lucru sigur, chiar și la distanță de rețeaua fizică din birou.

2

Politici și conformitate

Adaptează politicile companiei și nevoile de conformitate cu *best practices* pentru a răspunde amenințărilor cibernetice.

3

Awareness

Menține *focus* clar pe instruirea continuă în domeniul riscurilor de securitate cibernetică.

4

Suport

Pregatește un flux de suport capabil să raspundă la provocarile lucrului *remote-friendly.*

Tehnologie

1

Asigură un instrumentar tehnologic ce permite crearea unui mediu de lucru sigur, chiar și la distanță de rețeaua fizică din birou.

Wi-Fi Securizat
Asigură un nivel optim de conștientizare a practicii de a folosi o rețea WiFi Securizată în lucrul de acasă: **schimbarea denumirii implicite a rețelei, schimbarea parolelor implicite ale router-ului, update la cea mai recentă versiune firmware, utilizarea exclusivă WPA2/3**.

Share de documente și conferințe
Implementează un sistem de lucru cu o singură platformă colaborativă și asigură că informațiile importante NU sunt partajate între utilizatori și prin alte căi. **Folosiți o singură soluție de video conferencing.**

Acces și autentificare
VPN, 2 Factor Authentication, Anti-Malware pe fiecare dispozitiv, Data Leakage Prevention pe fiecare dispozitiv.

Politici si conformitate

2

Adaptează politicile companiei și nevoile de conformitate cu *best practices* pentru a răspunde amenințărilor cibernetice.

BYOD – Bring Your Own Device
Adaptează politicile de Securitate la realitatea BYOD. Angajații pot folosi și alte echipamente decât laptop-ul de la muncă. Creați cadrul necesar pentru a asigura măsuri de Securitate și pentru acele echipamente, ținând cont de diversitatea configurațiilor

Update, monitor & protect
Fluxurile operaționale de Securitate trebuie să funcționeze și în afara perimetrului fizic al companiei. SOC-urile vor avea vizibilitate asupra amenințărilor detectate pe endpoints, mecanismele de tip NAC vor restricționa accesul în rețea a device-urilor nesigure

Backup, Disaster Recovery
Politicile de backup și disaster recovery vor fi extinse pentru a include și informațiile din afara perimetrelor ‘tradiționale’

Awareness

3

Menține *focus* clar pe instruirea continuă în domeniul riscurilor de securitate cibernetică.

Instruire, Diseminare
Key factor: Extinde eforturile de training în privința securității informațiilor și în sensul includerii riscurilor asociate remote work-ului. Reiterează *focusul* companiei către prevenția incidentelor de Securitate printr-o bună diseminare a riscurilor asociate.

Noi bune practici
În contextul lucrului de acasă, o buna parte dintre angajati vor fi tentați să ignore politicile ce sunt aplicabile în mediul office, precum politici de tip clean desk, screen lockout sau schimbarea parolelor. Comunică importanță acestora

Social Media și *oversharing*
Comunica punctual riscurile asociate cu folosirea social media în contextul lucrului de-acasă. Oversharing-ul poate suplini, aparent, lipsa apropierii de la birou și rutina respectivă însa poate duce la scurgeri de informații.

Suport

4

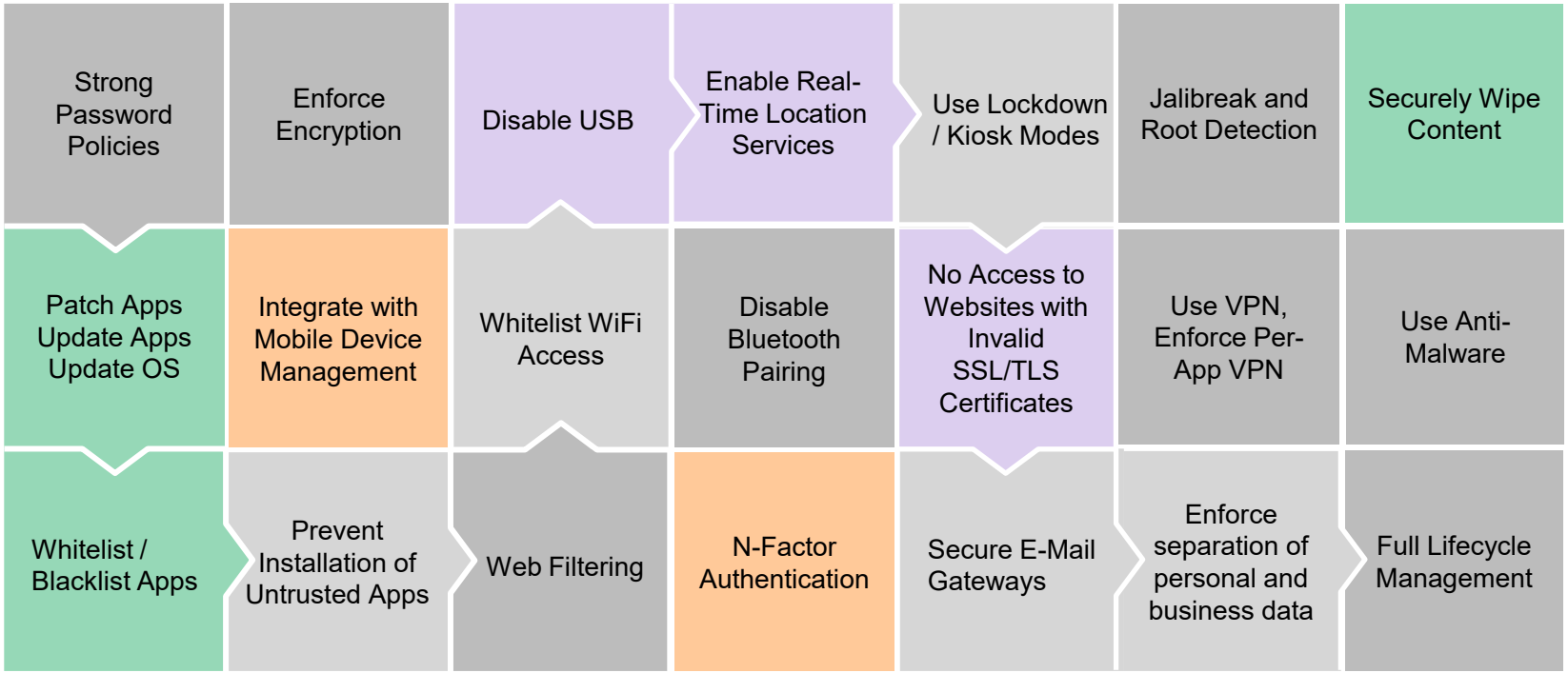
Pregatește un flux de suport capabil să raspundă la provocarile lucrului *remote-friendly.*

Monitorizare pro-activa a securității
Folosirea VPN pentru a accesa atât Internetul cât și resursele corporate aduce beneficiul vizibilității asupra traficului malițios. SOC-urile pot folosi, așadar, unelte de monitorizare a securității care permit intervenție în situația unor incidente de securitate

Help desk
Extinde fluxurile de suport pentru a include complexitatea remote work-ului: **BYOD, conexiuni nesigure, folosirea aceluiași device pentru muncă dar și în scop personal, expunerea la amenințări cibernetice ce nu pot fi mitigate la nivel de rețea**

Externalizați
Servicii profesionale precum SOCaaS și Managed Security pot prelua overhead-ul adus de remote work

Toolkit


Strong Password Policies
Enforce Encryption
Disable USB
Enable Real-Time Location Services
Use Lockdown / Kiosk Modes
Jalibreak and Root Detection
Securely Wipe Content
Patch Apps Update Apps Update OS
Integrate with Mobile Device Management
Whitelist WiFi Access
Disable Bluetooth Pairing
No Access to Websites with Invalid SSL/TLS Certificates
Use VPN, Enforce Per-App VPN
Use Anti-Malware
Whitelist / Blacklist Apps
Prevent Installation of Untrusted Apps
Web Filtering
N-Factor Authentication
Secure E-Mail Gateways
Enforce separation of personal and business data
Full Lifecycle Management

Business Internet Security Report

Get it from
www.threatmap.ro
or
www.orange.ro