Zero Trust Data Security

Luca Bechelli, CS Clusit

Andrea Brembilla, Sales Engineer, Rubrik

10 ottobre Verona 2023 orario 12.20-13.00

Luca Bechelli

COMITATO SCIENTIFICO CLUSIT

PARTNER @P4I – GRUPPO DIGITAL360

Andrea Brembilla

SALES ENGINEER @ RUBRIK

THREATS ARE EXPANDING

99%

of IT and security leaders were made aware of at least one attack in 2022. On average, **leaders dealt with attacks 52 times in 2022.**

59% experienced a data breach

54% BEC or fraudulent transfer

40% encountered ransomware

INTRUSIONS AFFECT OUR BUSINESS AND PEOPLE

93%

of external organizations encountering a cyberattack experienced a negative impact

42% LEADERSHIP FORCED TO CHANGE

49% Loss of customers

45% Revenue loss

44% Negative press and/or reputational damage

5% Stock negatively impacted

BACKUP ≠ CYBER RECOVERY

99%

of organizations reported having a backup and recovery solution

HOWEVER 93%
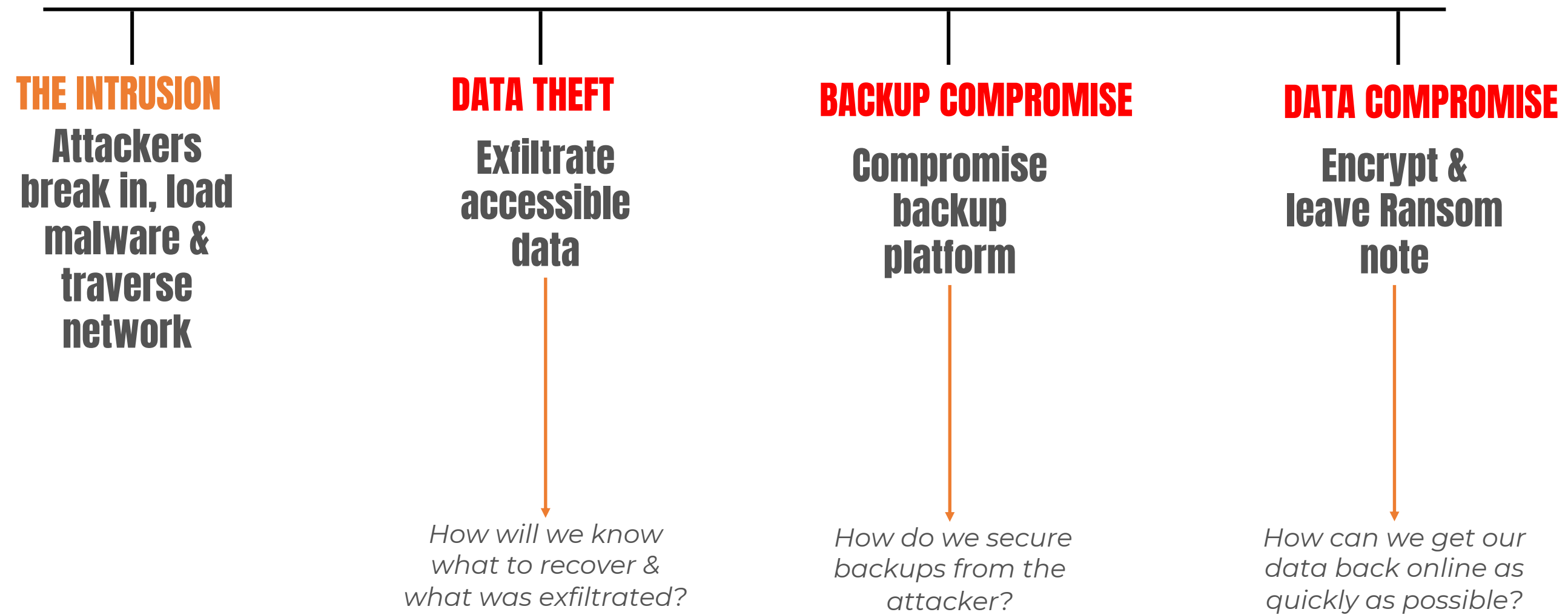
encountered significant issues with their solution

93%

of organizations reported malicious actors attempting to impact data backups

AND 73%

of these efforts were at least partially successful

FONTE: THE STATE OF DATA SECURITY, THE HARD TRUTHS (RUBRIK ZERO LABS, 2023)

Clusit
Associazione Italiana
per la Sicurezza Informatica

SECURITY SUMMIT
VERONA

rubrik

THE ANATOMY OF A RANSOMWARE ATTACK

THE INTRUSION

Attackers break in, load malware & traverse network

DATA THEFT

Exfiltrate accessible data

How will we know what to recover & what was exfiltrated?

BACKUP COMPROMISE

Compromise backup platform

How do we secure backups from the attacker?

DATA COMPROMISE

Encrypt & leave Ransom note

How can we get our data back online as quickly as possible?

Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY SUMMIT
VERONA

rubrik

ADOPT A ZERO TRUST APPROACH

Assume a breach will happen

Build Resilience   ✚   ### Continously Monitor   ✚   ### Respond

- Immutability is mandatory (but not enough)
- Multi Factor Authentication
- Encryption
- Air Gap
- And list goes on...

- Analyze anomalies as they happen
- Discover Sensitive Data Location
- Monitor Threats proactively
- Monitor Security preparedness

- Expedite mass recovery scenarios
- Build specific use cases for Cyber and Disaster Recovery
- Automate Recovery testing
- Leverage specific ransomware response team services

Q&A