RANSOMWARE. WHAT IS IT, WHY YOU SHOULD WORRY AND WHAT YOU CAN DO ABOUT IT.

Cheree, Pav and Geoff

NODE4

We are The Power People

We are The NAV People

We are The 365 People

WHAT IS RANSOMWARE?

"RANSOMWARE IS A TYPE OF MALWARE WHICH PREVENTS YOU FROM ACCESSING YOUR DEVICE AND THE DATA STORED ON IT, USUALLY BY ENCRYPTING YOUR FILES.

A CRIMINAL GROUP WILL THEN DEMAND A RANSOM IN EXCHANGE FOR DECRYPTION."

HOW RANSOMWARE WORKS

Example

Malware received via email/usb/web

The malware downloads malicious files (code)

The malicious code encrypts your data

You receive a ransom notice with a deadline

WHY WE ARE DISCUSSING THIS

246 Days	700mil	148%	44%	130
Average between infection & attack	Attempted attacks in 2021	Increase in attacks from 2020 to 2021	Of UK organizations said they were victims of an attack	Different strains detected

CUSTOMER STORIES

Customer A

- Lost everything
- Rebuilt their NAV system and data from 3 month old backup
- Took 4 weeks to get operational

Customer B

- Lost all systems and Data
- Had NAV and chose to reimplement Business Central instead
- Took 3 weeks to get up and running with BC
- Had to go to supplier and customers and ask what was owed
- Total estimated cost of lost revenue £9mil.

CUSTOMER STORIES

Customer C

- Group Penetrated systems
- Two levels of ransom
  - Fee to unencrypt data
  - Fee not to publicise attack to suppliers, customers and press
- Ransom paid at significant cost
- Systems were down for 1 week

Customer D

- Even with good security, backup and DR solutions in place were still down for 2 days with 1 day of data loss

“THE QUESTION IS NOT IF, BUT WHEN”

THINGS TO CONSIDER

Prevention

- Email security and web filtering
- Training for Staff
- Endpoint Detection and Response
- Identity and Access Management
- Vulnerability Management
- Onboarding and outboarding

THINGS TO CONSIDER

Recovery

- Planned and measurable recovery strategy
- Backup storage immutability
- Make sure you have an off-network backup
- Plan for an attack
- Regular test of backups
- Key resources and contacts outside system

RECOVERY - NAV VAULT

- Business continuity beyond existing backups
- Provides an air-gapped, off-site backup service
- Provides secure NAV/BC environment
- Daily incremental SQL database backup
- Weekly restore of SQL backup up database onto a dedicated NAV/BC system
- Environment is managed, monitored and check-up regularly

PREVENTION - DR DOCTOR

- Free 1 hour DR Health Check session
- What is covered:

  - Discussing Cloud Strategy across the business
  - Understand key business applications
  - Where these business applications are deployed
  - The extent to which vulnerability is being minimised
  - How long will it likely take to recover

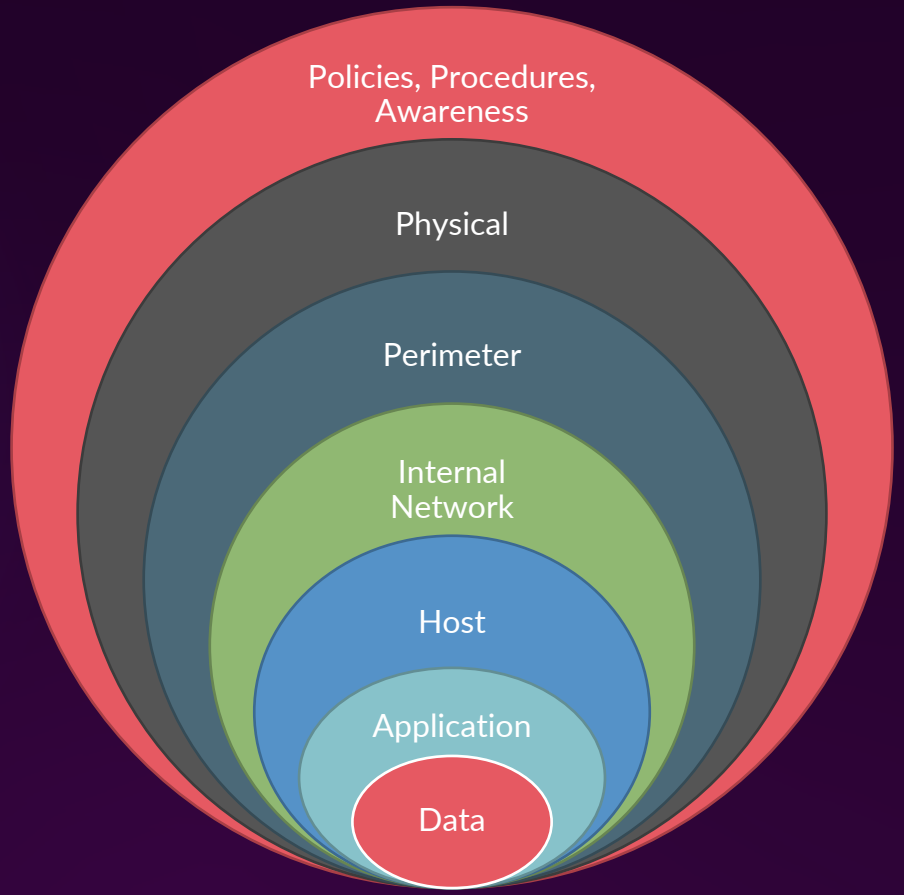
  Output: List of layered recommendations; quick fixes, medium and long term

NODE4

There is no single method of preventing ransomware

You should assume some malware will enter your network at some point

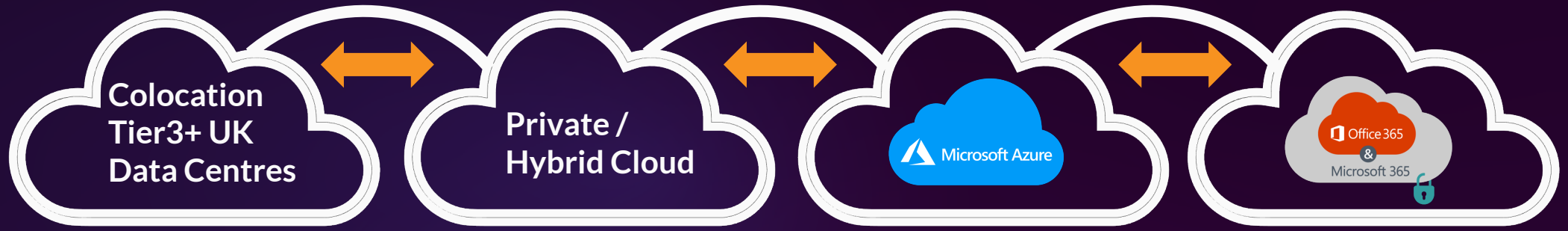
A ‘defence in depth’ approach is required to limit impact and improve response time



NODE4

Hybrid Cloud Managed Services and Integrated Support (24x7 Service Desk / NOC / SOC)

Colocation / Hosted | Private Cloud Services | Public Cloud Services



Colocation

Infrastructure as a Service

Platform / Software as a Service

Data, Applications and Security Management Services

SD-WAN & MPLS Network / Connectivity Services

Backup as a Service / Disaster Recovery as a Service

We are The Power People

We are The NAV People

We are The 365 People

NEXT STEPS

- Visit the Node4 stand
- Sign up for our DR Doctor Service
- Speak to your TNP Engagement Management for further information about Node4 services

Q&A