ezAccount

Improving network security in a tax accountant office

RISK MANAGEMENT & NETWORK SECURITY ANALYSIS

PREPARED FOR

Family-run accountancy firm

Yair **Levy** • Federico **Niccolini**

Emanuele **Urselli** • Gianmarco **Pastore** • Alessandro **Zanatta** • Sergio **Parigi** • Andrea **Vergori**

ezAccount - Improving network security in a tax accountant office
Introduction

TEAM 1

Objectives
Mitigate cybersecurity risks and improve the overall security of a tax accountant firm, ezAccount

ezAccount current situation
Tax accountant with 5 employees
2 offices in Tampa and S. Petersburg
Offers financial, accounting and taxation services

Problems
Lack of business continuity, incident response, and recovery plan
It has some security issues related to the network and staff training

ezAccount - Improving network security in a tax accountant office

Recognize and define the problem

TEAM 1

Cybersecurity in tax accounting SMEs
Management of sensitive data
Shift towards digital and cloud services
Dangers deriving from: collaboration with insecure third parties, network vulnerabilities, phishing, social engineering, compromise of company emails.
Lack of in-house skills (Parkin et al., 2016, 1-2)
Impact of an attack both on owner and clients
Increase in the number of cyber attacks during Covid-19 (Lallie et al., 2021, 3-11)

ezAccount - Improving network security in a tax accountant office

Gather facts

TEAM 1

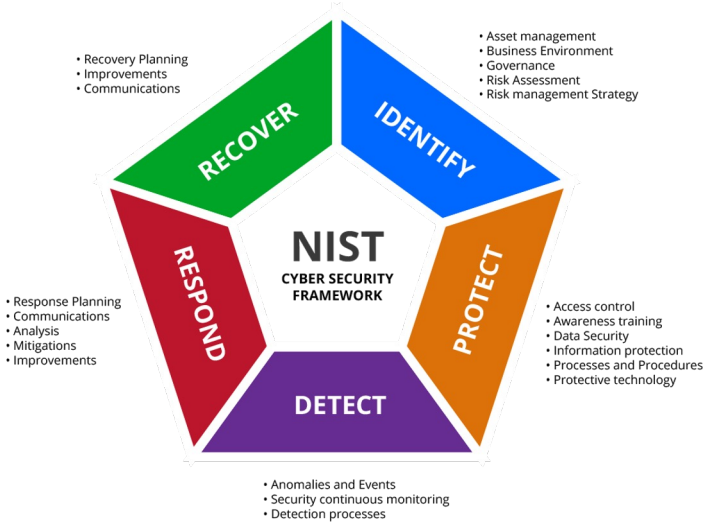
Current technical situation of ezAccount firm
2 offices with a NAS on each
Cloud-based applications for tax accountancy
Shared Wi-Fi and unrestricted usage of personal devices
Pinned passwords
Remote connection via standard OS VPN
Many devices connected to the network (printers, security cameras)
Tier 1 of NIST cybersecurity framework

ezAccount - Improving network security in a tax accountant office
Project scope, goals, and objectives

TEAM 1

Project scope
Managerial problems (cyber-hygiene, cyber-awareness)
Technical aspects (network defense)

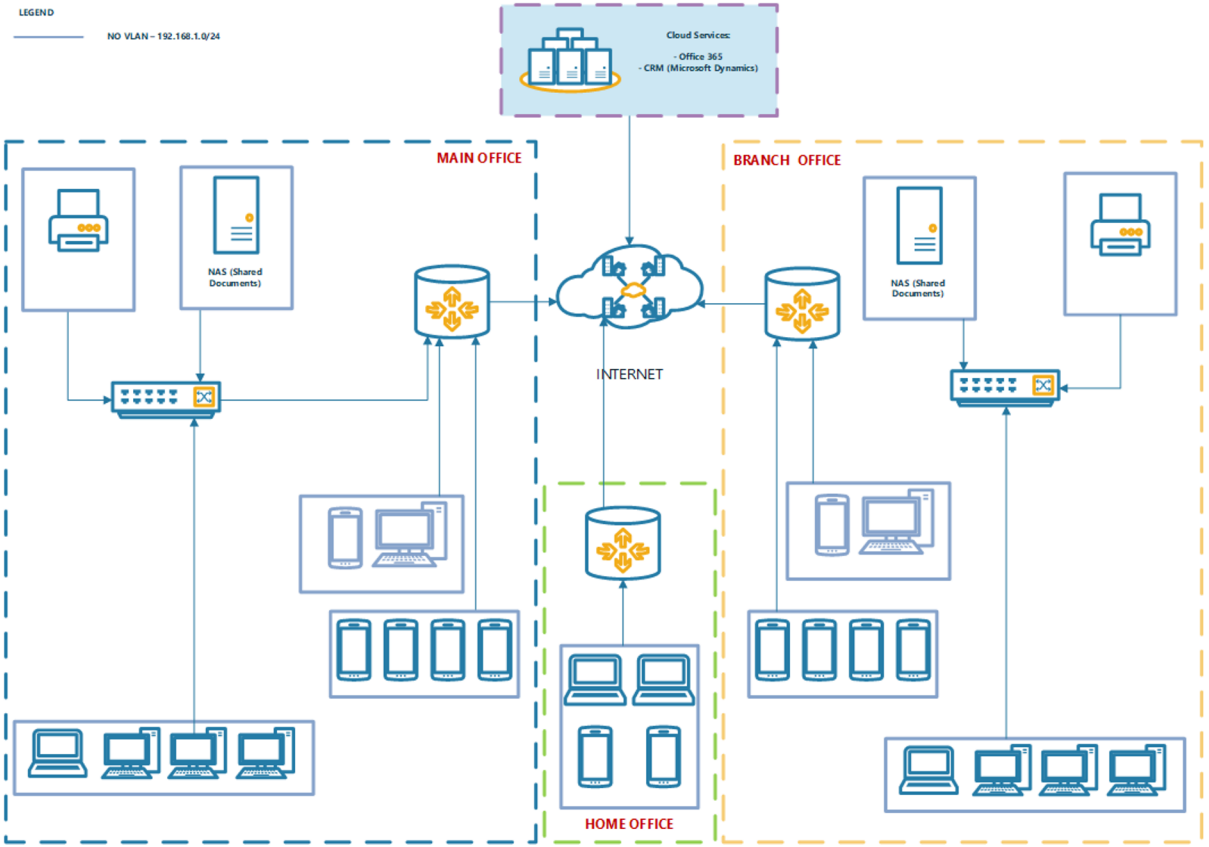
Objectives
Efficient and safe network architecture (firewalls, VPN, centralized antivirus, IDs)
Mitigate lack of encryption or unsafe access control policies
Train employees and managers, establishing an IRP and a BCP.



ezAccount - Improving network security in a tax accountant office

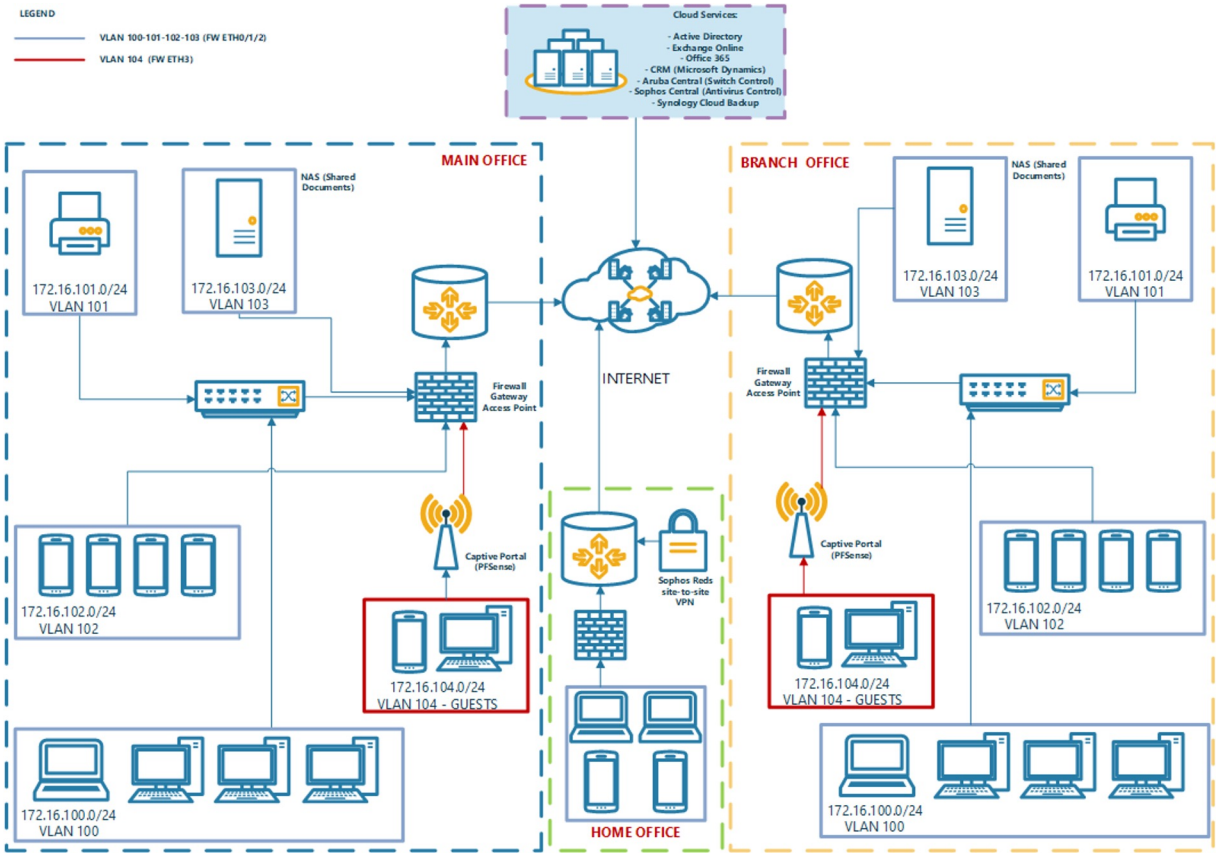
Proposed Solution - Before network improvement

TEAM 1



ezAccount - Improving network security in a tax accountant office
Proposed Solution - After network improvement

TEAM 1



ezAccount - Improving network security in a tax accountant office
Action plan (Part 1)

TEAM 1

ACT_#	Item	Description	Type	NIST Category

ACT-1	Firewall Installation for both offices, proxy configuration for web site access segmentation, Adoption of VPN with strong encryption. Intrusion detection system (IDS) activation	• Buy two (Sophos Firewall). Implement the follow features:
		  ◦ Configure Firewall Policies
		  ◦ Configure Web Proxy used by company users
		  ◦ Configure site-to-site VPN and install VPN software client on the CEO Laptop
		• Buy one (Sophos RED) for home security connected to Office Firewalls using a fixed VPN connection
		• Buy one Bitdefender Box Firewall (@ CEO Home)
		• Buy two HPE Managed Switch (24 ports)
		• Configure different VLAN for every type of device (wireless, printers, PC and NAS, captive portal)
		• Install Servers/Network Secure Cabinet
		• Buy two enterprise level NAS (Synology RS Series) synchronized by a Synology service. Home can reach the main nas using VPN connection
		• All NAS data will be saved on cloud using Synology C2 Backup service
		• Buy a BYOD cloud system (Cisco Meraki)
		• Install PFSense Captive Portal Appliance
			Technical	PR-AC

		• Configure the IDS (Intrusion Detection System)	Technical	DE.AE
		• Buy a (Sophos) Central Antivirus for every device of the organization	Technical	DE.CM
ACT-2	Employee training about cyber-hygiene and cyber-awareness	• Manager training • Employee training	Managerial	PR.AT

ezAccount - Improving network security in a tax accountant office
Action plan (Part 2)

TEAM 1

ACT_#	Item	Description	Type	NIST Category
ACT-3	Create Business Continuity (BC) and Incident Response (IR) Plan	• Define disaster recovery procedure • Setup Emergency Contact list • Employee Training • Configure automatic security updates	Managerial Technical	RC.RP
		• Implements a Maintenance Program (update/security fix)	Technical	PR.MA
		• Define Response procedure	Managerial	RS.CO
		• Detailed assets of hardware & software and business data flow	Managerial	ID.AM
ACT-4	Use of data encryption on every asset, data synchronization on the cloud. Enroll all mobile devices to BYOD manager. Least privilege configuration, implementation of role-based access control (RBAC), zero-trust authentication and/or 2FA	• Configure data encryption on each device • Implement backup strategies on BYOD • Configure Two-Factor authentication • Configure Role Based Access Control on NAS	Technical	PR-DS

ezAccount - Improving network security in a tax accountant office
Risk Management Analysis (RMA) outline

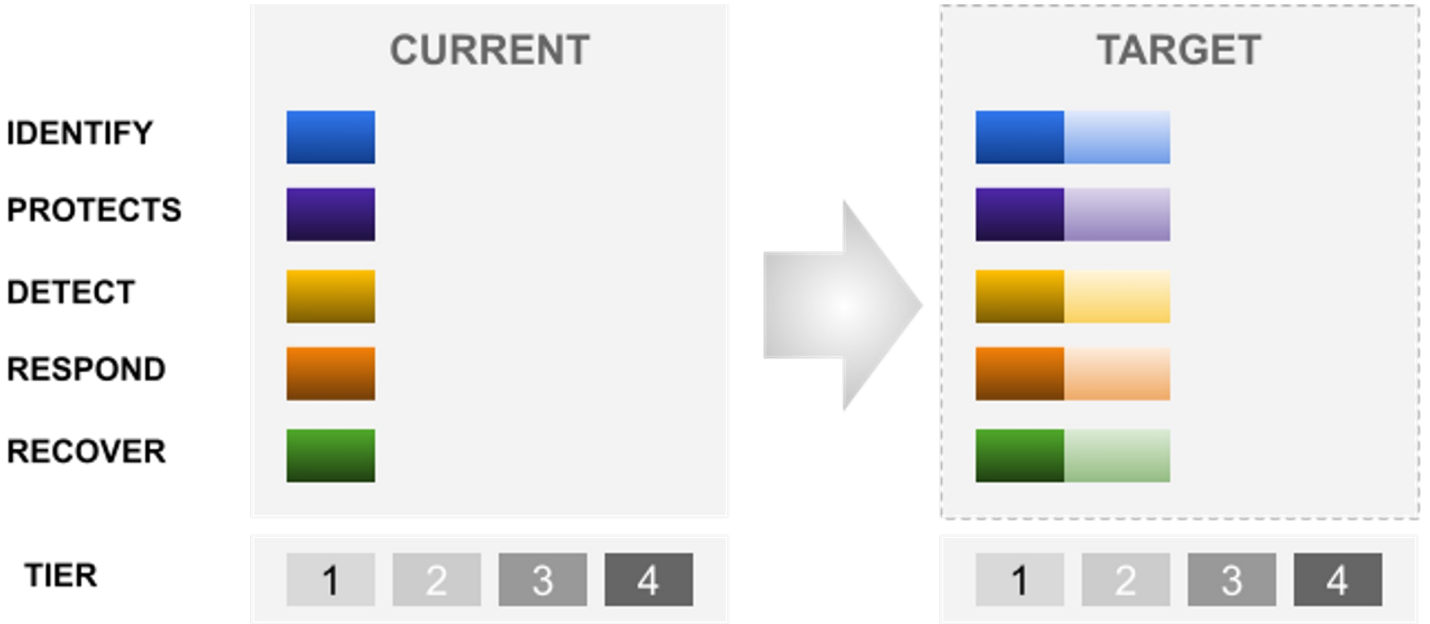
TEAM 1

Risk rank	Threat type	Risk description	Likelihood of occurrence	Impact on organization	Mitigation strategy	ACT_#
1	Data breach	Unauthorized disclosure of sensitive customer data, due to data breach	HIGH	HIGH	Firewall Installation for both offices, proxy configuration for web site access segmentation, Adoption of VPN with strong encryption. Intrusion detection system (IDS) activation	ACT-1
2	Ransomware	Network modification, loss of productivity, files and financial loss as a result of revenue generating operations being shut down or/and paying ransom	HIGH	HIGH	Employee training about cyber-hygiene and cyber-awareness, use of RAID 5, antivirus, disable macro scripts, use of server proxy for internet access	ACT-2
3	Data leakage	Loss of data confidentiality, communication confidentiality due to data leakage	MEDIUM	HIGH	Adoption of VPN with strong encryption	ACT-1
4	Unauthorized Remote Access	Loss of confidentiality, integrity and availability. due to unauthorized remote access	MEDIUM	HIGH	Least privilege configuration, implementation of role-based access control (RBAC), zero-trust authentication and/or 2FA	ACT-4
5	Network breach	Loss of confidentiality due to network breach	MEDIUM	HIGH	VLAN adoption, installation of a captive portal on a dedicated VLAN	ACT-1
6	Business Operation continuity/recovery risk	Business operation disruption and potentially bankruptcy due to the lack of business continuity plan / Incident Response Plan	LOW	HIGH	Create Business Continuity (BC) and Incident Response (IR) Plan	ACT-3
7	Physical access	Loss of backup data files due to theft of hardware or sabotage	LOW	HIGH	Use of data encryption on every asset, data synchronization on the cloud. Enroll all mobile devices to BYOD manager	ACT-4

ezAccount - Improving network security in a tax accountant office

Anticipated project results

TEAM 1



ezAccount - Improving network security in a tax accountant office
Proposed Costs - Non Recurring Cost

TEAM 1

Activity list

Action	ACT-REF	Hours	Cost/Hour	Price
Configure Firewall Policies	ACT-1	4	€ 100	€ 400
Configure Navigation Proxy used by company users	ACT-1	4	€ 100	€ 400
Configure the Intrusion Detection System (IDS)	ACT-1	4	€ 100	€ 400
Install and configure VPN client to all devices	ACT-1	6	€ 100	€ 600
Configure different VLAN for every device	ACT-1	2	€ 100	€ 200
Configure NAS on cluster mode	ACT-1	4	€ 100	€ 400
Manager and employee training	ACT-2	4	€ 100	€ 400
Define recovery procedure	ATC-3	4	€ 100	€ 400
Setup Emergency Contact list	ATC-3	2	€ 100	€ 200
Configure automatic security updates	ATC-3	2	€ 100	€ 200
Implements a Maintenance Program	ATC-3	4	€ 100	€ 400
Configure data encryption on each device	ATC-4	8	€ 100	€ 800
Implement backup strategies on BYOD	ATC-4	4	€ 100	€ 400
Configure 2 factor authentication	ATC-4	4	€ 100	€ 800
Configure Role Based Access Control on NAS	ATC-4	6	€ 100	€ 600

TOTAL ACTIVITIES	€ 6.600

Start-up material list

Item	ACT-REF	Qty	Unit Price	Price
Sophos XGS Firewall	ACT-1	2	€ 300	€ 600
Bitdefender box firewall	ACT-1	1	€ 250	€ 250
Sophos RED	ACT-1	1	€ 350	€ 350
HPE Aruba 2930F	ACT-1	2	€ 2.250	€ 4.500
Servers/Network Secure Cabinet	ACT-1	2	€ 200	€ 400
(Sophos) Central Antivirus	ACT-1	1	€ 100	€ 100
Synology RS 819 + DISKS	ACT-1	2	€ 1.650	€ 3.300

TOTAL MATERIAL	€ 9.500

TOTAL COST	€ 16.100

ezAccount - Improving network security in a tax accountant office
Proposed Costs - Recurring Yearly

TEAM 1

Activity Maintenance List

Action	ACT-REF	Hours	Cost/Hour	Price
Configure Firewall Policies	ACT-1	1	€ 100	€ 100
Configure Navigation Proxy used by company users	ACT-1	1	€ 100	€ 100
Configure the IDS (Intrusion Detection System)	ACT-1	1	€ 100	€ 100
Maintenance of the recovery procedure	ATC-3	4	€ 100	€ 400
Setup Emergency Contact list	ATC-3	1	€ 100	€ 100

RECURRING ACTIVITIES (YEARLY)	€ 800

Recurring Cost (yearly) Material List

Item	ACT-REF	Qty	Unit Price	Price
Sophos FW annual maintenance	ACT-1	1	€ 1.000	€ 1.000
Aruba Central (3 years subscr)	ACT-1	1	€ 200	€ 200
(Sophos) Central Antivirus	ACT-1	1	€ 500	€ 500
Synology Cloud C2 Backup	ACT-1	1	€ 99	€ 99
Synology Cloud C2 Storage	ACT-1	1	€ 139	€ 139

RECURRING MATERIAL (YEAR)	€ 1938

TOTAL COST	€ 2738

The proposed project
Ensures greater confidentiality and integrity of the resources
Improves the company ability to respond and recover from an incident
Involves an investment of **18838$** and **70h** to make the company risk-informed
Achieves NIST tier 2

ezAccount - Improving network security in a tax accountant office
References

TEAM 1

Barrett, M. P. (2018). *Framework for Improving Critical Infrastructure Cybersecurity* (1.1). NIST Cybersecurity Framework. https://doi.org/10.6028/NIST.CSWP.04162018

Fernandez De Arroyabe, I., & Fernandez De Arroyabe, J. C. (2021). *The severity and effects of Cyber-breaches in SMEs: a machine learning approach*. Enterprise Information Systems. 10.1080/17517575.2021.1942997 To link to this article: https://doi.org/10.1080/17517575.2021.

IRS warns about COVID-19 economic impact payment fraud. (2021, June 4). Internal Revenue Service. Retrieved November 24, 2021, from https://www.irs.gov/compliance/criminal-investigation/irs-warns-about-covid-19-economic-impact-payment-fraud

Lallie, H. S., Shepherd, L. A., Nurse, J. R.C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021, June). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*(1), 102248. 10.1016/j.cose.2021.102248

Parkin, S., Fielder, A., & Ashby, A. (2016). *Pragmatic Security: Modelling IT Security Management Responsibilities for SME Archetypes*. 10.1145/2995959.2995967

THANK YOU

for your precious time and attention