

Microsoft Attack Simulation Training powered by sepago

Customer Case Study

SEPAGO IN A NUTSHELL



SYSTEM INTEGRATOR, ISV AND CLOUD MANAGED SERVICE PROVIDER



SINCE 2002

SUCCESSFUL ON THE MARKET AT THREE LOCATIONS: COLOGNE HAMBURG MUNICH





SPECIALISED IN

MICROSOFT CLOUD TECHNOLOGIES, MODERN WORKPLACE, MOBILITY, APP VIRTUALISIERUNG & VDI, CITRIX WORKSPACE APP, VIRTUAL MANAGED SERVICES, IT CHANGE MANAGEMENT & IT-SECURITY



HUNDREDS OF SATISFIED CUSTOMERS



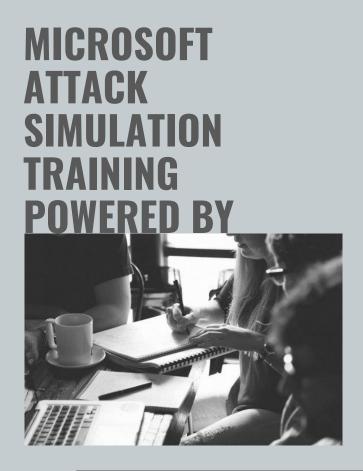
85 ENTHUSIASTIC EMPLOYEES

EXCELLENT ORGANIZATIONAL CULTURE COMMUNITY AWARDS



MILLIONS OF GOOD IDEAS





sepago accompanies the pre-operation
phase continuously and in a procedurally
structured manner based on blueprints and
templates to set-up the Microsoft Attack
Simulation Training for efficient and effective
cyber security phishing campaigns.



THE COMPANY

- small, Germany-based automotive manufacturing company (MDAX-based)
- 25.000 employees generated about 2,5 billion € in 2020

Current Challenge:

Customer has just introduced new Microsoft 365 Defender suite. But their employees are not yet mature enough to recognize malicious emails and files, attacks are prevented by the Defender solutions.

The CISO wants to implement an Attack Simulation Training, but does not know, how and where to start.





WHAT WE DELIVERED

Using the Microsoft Attack Simulation Training included in Microsoft Defender for Office, we have guided the customer through the trainings:

- I. Structured campaigns with a security phishing awareness process.
- II. The right training materials in the right context for the right people.
- III. The interpretation of the campaign results and appropriate next steps.



AGENDA OF THE ENGAGEMENT

Kick-off-Phase

- Tool demo
- Process assessment
- End-user Reward model

Monitoring & metrics set-up

- Measurement plan/ Scorecard
- Dashboard implementation
- API connection to Microsoft PowerBI

Process & Implementation guidance

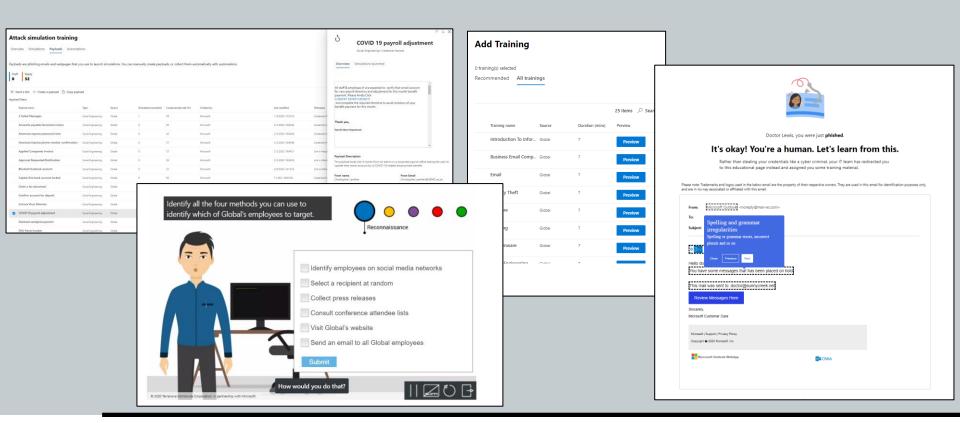
- Development & documentation operational model/ process
- Development & documentation technical Implementation plan
- Development Phishing Awareness Communication plan & material
- Roll-out Microsoft Attack Simulation & Training

Continuous support in Microsoft Attack Simulation & Training

- Initial campaign set-up
- Continuous campaign set-up
- Monitoring of results
- Recommendations of improvements & next steps



MICROSOFT ATTACK SIMULATION TRAINING





GUIDANCE BY SEPAGO

- 1_MicrosoftAttackSimulator.docx
- Implementation_ _PM (export).xls
- Implementation_Communicationplan.xlsx
- Implementation_Transformationmap.pptx
- MicrosoftAttackSimulator.docx
- Process_Campaignplan.xlsx
- Process_End-user survey.xlsx
- Process_Improvementlist.xlsx
- Process_Layer1_HighLevel.vsdx
- Process_Layer2_Action Items_process.xlsx
- Process UX measurement plan.xlsx

Content					
1	Introduction				
2	Implementation: Transformation map & Gantt-diagram				
3	Impl	ementation: Removal guide for Cofense button	8		
	3.1	Removing the Add-In for All Users inside Office 365	9		
	3.2	Removing the Add-In for All Users inside Exchange 201X	10		
4	Impl	ementation: Implementation guide for report-add in	11		
	4.1	Implementing the Report Message add-in by Microsoft	11		
	4.2	User submission policy	13		
5	Impl	ementation: Report Dashboard in SharePoint	18		
6	Impl	ementation: Communication plan	18		
7	Impl	ementation: Communication material	19		
	7.1	SharePoint text end-user	19		
	7.2	Yammer Announcement text end-user & DW early adopter	22		
	7.3	Email notification end-user	23		
	7.4	Announcement text Cyber Defence Team/Operational teams	24		
	7.5	Reminder Announcement text Operational teams & function guide	27		
8	Proc	ess	28		
9	Proc	ess: Visio high-level	29		
10	Proc	ess: Action Items & step-by-step	30		
	10.1	Preparation yearly (Trigger: calendar year)	30		
		10.1.1 Editorial calendar.	30		
		10.1.2 Campaign plan (document)	33		
	10.2	Campaign monthly (Trigger: calendar month)	33		
		10.2.1 Choose topic based on campaign plan			
		10.2.2 Check targeted AD group	34		

		10.2.3 Check education landing page	35
		10.2.4 Test run	36
		10.2.5 Set-up campaign in Attack Simulator	37
		10.2.6 Inform necessary stakeholder	40
		10.2.7 Campaign runs for 7 days	42
	10.3	Campaign review monthly (Trigger: end of campaign/month)	43
		10.3.1 Share PowerBI report on SharePoint	43
		10.3.2 Meeting to review the last campaign if required	44
	10.4	Extra processes: Awareness & service review (Trigger: calendar year)	46
		10.4.1 Process: Continuous reporting, review & improvement process	46
11	Micro	osoft Attack Simulator documentation	48
	11.1	Attack Simulator Overview	48
	11.2	Step-by-Step: Creating a custom payload.	50
	11.3	Step-by-Step: Creating/Scheduling a Simulation	54
	11.4	Step-by-Step: Cancel a scheduled simulation.	59
12	Proc	ess: Campaign plan Q3+Q4 2021	60
13	Proc	ess: Communication templates & material	61
	13.1	Test information mail	61
	13.2	Info Mail Stakeholder	
	13.3	Landing page educational	63
		FAO Phishing	
	13.5	Header/Body training	67
15		ard for compliance model	
		user survey for sentiment analysis	
17		ess: Monitoring	
		Measurement plan & end-user KPI structure	
	17.2	Process monitoring in PowerBI	71

OUTCOME FOR THE CUSTOMER

- Compared to before the engagement, we were able to reduce the amount of employees clicking on malicious files and mails by 45%
- Employees liked the approachable and personal training experience and the gamification aspect
- Security operations resources can be allocated to different cyber defence areas – less noise in Microsoft Defender 365





THANK YOU FOR YOUR **ATTENTION!**

Let us hear from you!









