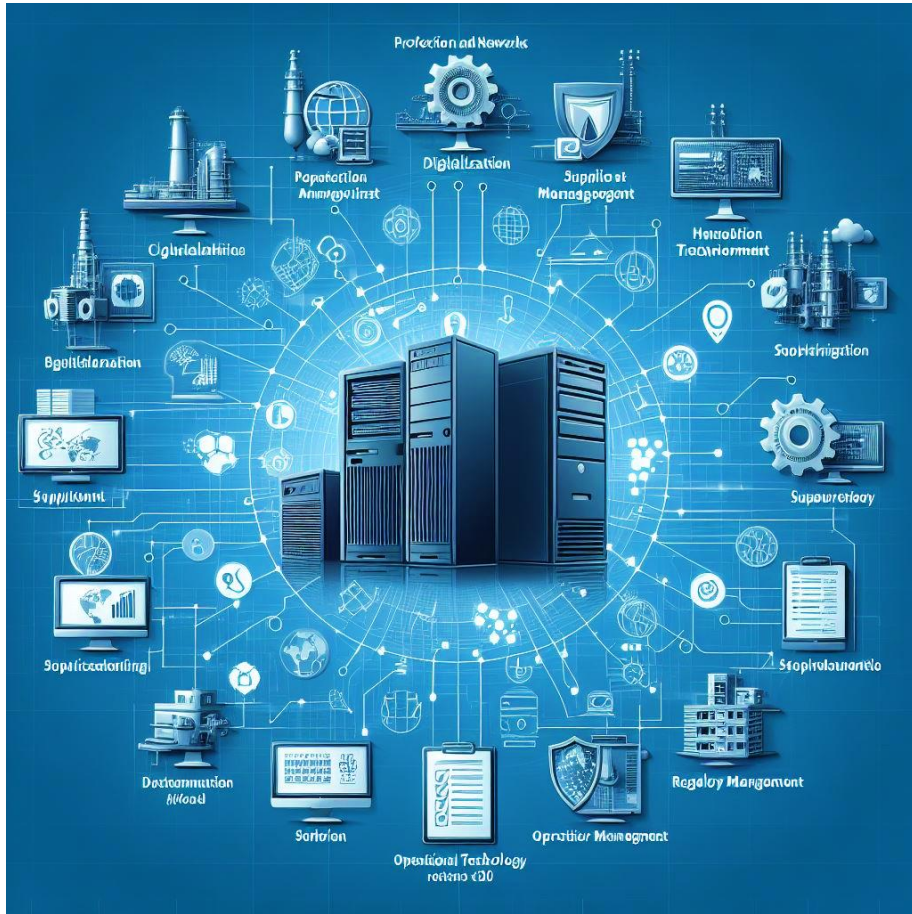


Cybersécurité dans une entreprise de transports publics

5 juin 2024, BUS 24

Thomas Kolly, responsable Informatique de BERNMOBIL

Défis



Protection contre les cyberattaques



Numérisation

1010
1010

Gestion des fournisseurs



Technologie opérationnelle



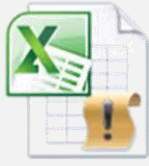
Défis réglementaires



Activités

Techniques

Client /
utilisateur



Macros



Antivirus



Authentification multifacteur



Cryptage des
documents HD

Systèmes



Pare-feu
DDoS



Filtre spam
e-mail



Scan/patch des
points faibles



Backup



Identity
Access
Management



Privileged
Access
Management

Surveillance



Accès
Autorisations



Analyse LOG



Monitoring de la protection
des points finaux



Pentest
TP + app/véhic.



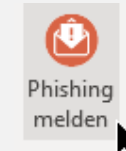
Périmètre

Organisationnelles

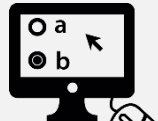


SCHPÄÄM
KOPF BENÜTZEN, DATEN SCHÜTZEN

Sensibilisation des collaborateurs



Outlook /
smartphone



Dashboard
module
d'apprentissage



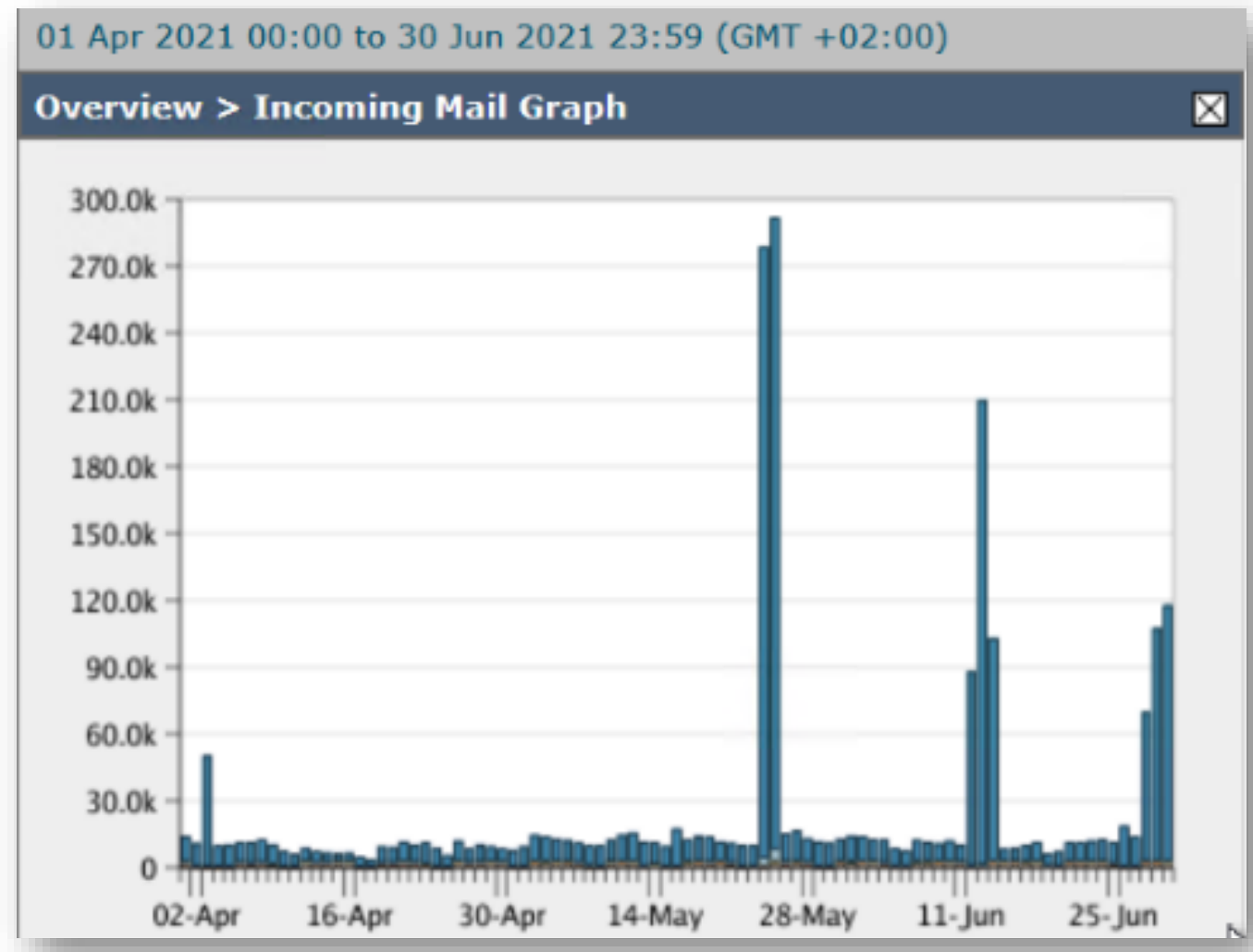
Directives IT



Mot de passe

Évaluation du filtre spam e-mail (T2 2021: 1^{er} avril – 30 juin 2021)

Overview > Incoming Mail Summary		
Message Category	%	Messages
Stopped by Reputation Filtering	90.3%	2.0M
Stopped as Invalid Recipients	0.9%	19.0k
Spam Detected	0.6%	13.9k
Virus Detected	0.0%	3
Detected by Advanced Malware Protection	0.0%	3
Messages with Malicious URLs	0.0%	37
Stopped by Content Filter	0.0%	215
Stopped by DMARC	0.5%	11.4k
S/MIME Verification/Decryption Failed	0.0%	0
Total Threat Messages:		
	91.9%	2.0M
Marketing Messages	0.9%	20.2k
Social Networking Messages	0.2%	4,611
Bulk Messages	1.0%	21.4k
Total Graymails:		
	2.1%	46.2k
S/MIME Verification/Decryption Successful	0.0%	0
Clean Messages	6.0%	130.2k
Total Attempted Messages:		
		2.2M



Test de pénétration Bus

Bus articulé hybride Volvo 7900 A 2^e gén

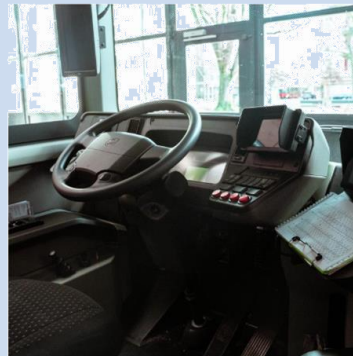
29 bus articulés hybrides Volvo circulent sur le réseau de BERNMOBIL



Volvo Hybrid-Gelenkbus im Depot



Der Volvo Hybridbus von Innen



Der Führerstand des Volvo 7900 CS92

Länge des Fahrzeugs	Breite des Fahrzeugs	Höhe des Fahrzeugs	Leergewicht
18'740 mm	2'550 mm	3'300 mm	18,8 t
Kapazität	Maximale Geschwindigkeit	Lieferjahre	Typenblatt
148 Personen (37 ♿)	80 km/h	2022	<u>PDF</u> 1.07 MB

Problématique

- Test de pénétration effectué à l'externe à l'aide de la méthode de la boîte noire et de cas d'application ciblés

Objectif

- Identifier des points faibles techniques du matériel, des logiciels, des interfaces y c. télématique du véhicule et des réseaux liés au bus interconnecté

Conditions-cadres

- Le même véhicule pendant tout le test de pénétration, pas d'enregistrement de l'interface de communication mobile, non destructif, accès au système de télématique / Volvo Connect interdit par le constructeur

Test de pénétration Bus: cas d'application

Système ITCS (système de commande)

- Ordinateur de bord
- Terminal de commande au poste de conduite
- Écrans avec «collier de perles»
- Affichages extérieurs (ligne, destination)

Système de publicité

- Routeur
- Écrans avec publicité

Comptage des passagers

- Collecteurs de données de mesure
- Capteurs aux portes

Systèmes du constructeur du véhicule

- Commandes des composantes du véhicule (moteur, portes, bus CAN, etc.)
- Système de télématique

Test de pénétration Bus: résultats

Schwachstelle	Verantwortl. Organisation			Gefährdete Systeme			Prio
	BERNIMOBIL	Trapeze	APS	Bordrechner	Werbesystem	Terminal IPT	
Ungeicherter Zugang zum Netzwerk		x	x	x	x	x	1
Access Control - Fehlende oder unzureichende Authentifizierungsprüfung		x		x	x	x	1
Local File Inclusion		x		x	x		1
End of Life von Soft- oder Hardware		x	x	x	x	x	1
Denial of Service (DoS)			x		x		1
Command Injection / Remote Code Execution (RCE)		x			x	x	2
"Lateral Movement" - Eskalation der Rechte		x		x	x		2
Sensitive Informationen im Klartext gespeichert		x	x	x	x	x	2
Unzureichender Schutz gegen Schadsoftware		x	x	x	x		2
Verwendung unsicherer Netzwerkprotokolle - HTTP		x		x	x	x	2
Klartextübertragung sensibler Informationen - FTP Server Klartextauth.			x		x		2
Verwendung unsicherer Netzwerkprotokolle - (SMB) Protocol Version 1		x		x	x		3
User Enumeration		x	x	x	x		3
Schwache Passwort Richtlinien	x	x		x	x	x	3
Fehlende SMS-Sicherheitsmaßnahmen		x		x	x		3
Veralterte oder ungepatchte Software		x		x	x		3
Unzureichende Firewall-Regeln		x	x	x	x	x	3
Offene Ports und erreichbare Dienste		x	x	x	x	x	3
Informationsgewinn		x		x	x		3

Phishing Awareness Dashboard



BERNMOBIL
ZUSAMMEN UNTERWEGS

Logout

Ihre persönliche Statistik

9

Simulation
erhalten

0

Simulation
angeklickt

0

Simulation
gescheitert

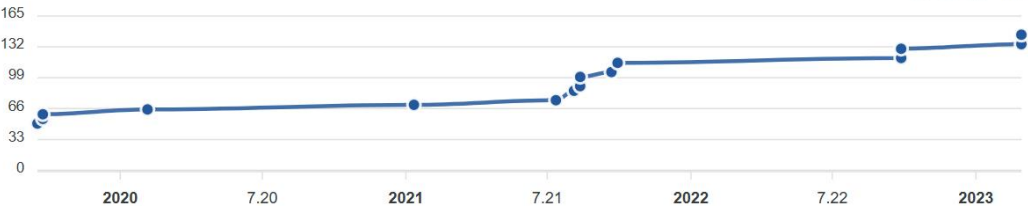
5

Simulation
gemeldet

0

Bösartige
E-Mails
gemeldet

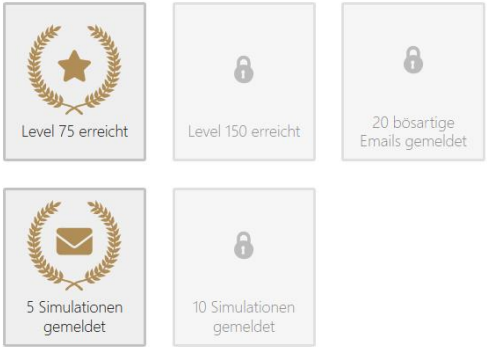
Ihre Leistung



Ihr Fortschritt



Ihre Erfolge



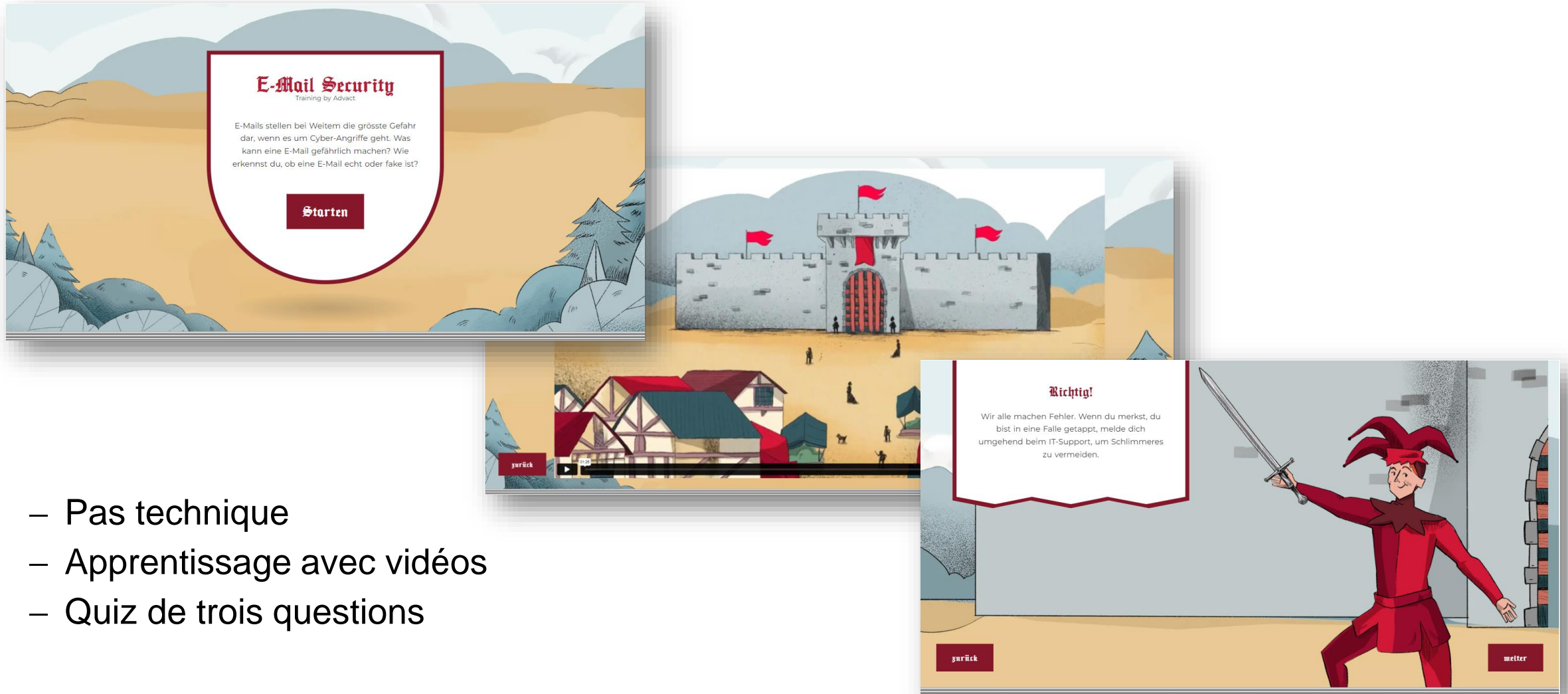
Rangliste

Ihr persönliches Level Unternehmenslevel

145 0

Rang	Von	Level	Beste/er	Schlechteste/er
9	1413	145	165	0

Module d'apprentissage sur le hameçonnage



- Pas technique
- Apprentissage avec vidéos
- Quiz de trois questions

Que faisons-nous d'autre?

Analyse de risques IT

- Analyse intégrale des risques IT tous les 3 ans
- Vérification annuelle

NCSC/BACS – cercle de clients fermé

- Accès au Cyber Security Hub
- Informations pour la propre organisation
- Alerte en présence d'un message
- Offre de prestations (GovCERT.ch)

Board ISMS

- Lancement
- Mesures de base
- Monitoring et contrôle

Cellule de crise

- Cybersécurité
- Exercice «au ralenti»

Conclusion

- La cybersécurité nous occupe beaucoup et continuera à le faire
- Les cyberattaques ne sont pas de la fiction, mais la réalité
- Lutter contre les cyberrisques nécessite des mesures tant techniques qu'organisationnelles
- L'humain est à la fois le plus grand facteur de risques et de protection

Nous voyons la sécurité de l'information non pas comme un état, mais comme un processus, car il n'y a pas de sécurité de l'information à 100 %.

La cybersécurité dans les entreprises de transports publics est décisive pour protéger les infrastructures critiques et garantir une exploitation sûre et fiable.

