



Cyber-Sicherheit im öV-Unternehmen

5. Juni 2024, BUS 24

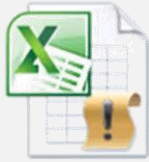
Thomas Kolly, Leiter Informatik BERNMOBIL



Aktivitäten

Technisch

Client /
Anwender



Makro



Antivirus



Multi Factor Authentication

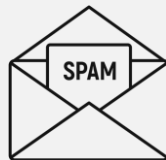


Verschlüsselung HD
Dokumente

Systeme



Firewall
DDoS



E-Mail
Spamfilter



Schwachstellen
Scan/Patch



Backup



Identity
Access
Management



Privileged
Access
Management

Überwachung



Zugriffe
Berechtigungen



LOG-Analyse



Endpunktschutz
Monitoring



Pentest
öV+ App/Fz



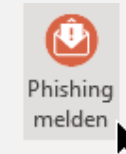
Perimeter

Organisatorisch



SCHPÄÄM
KOPF BENÜTZEN, DATEN SCHÜTZEN

Sensibilisierung Mitarbeitende



Outlook /
Smartphone



Dashboard /
Lernmodul



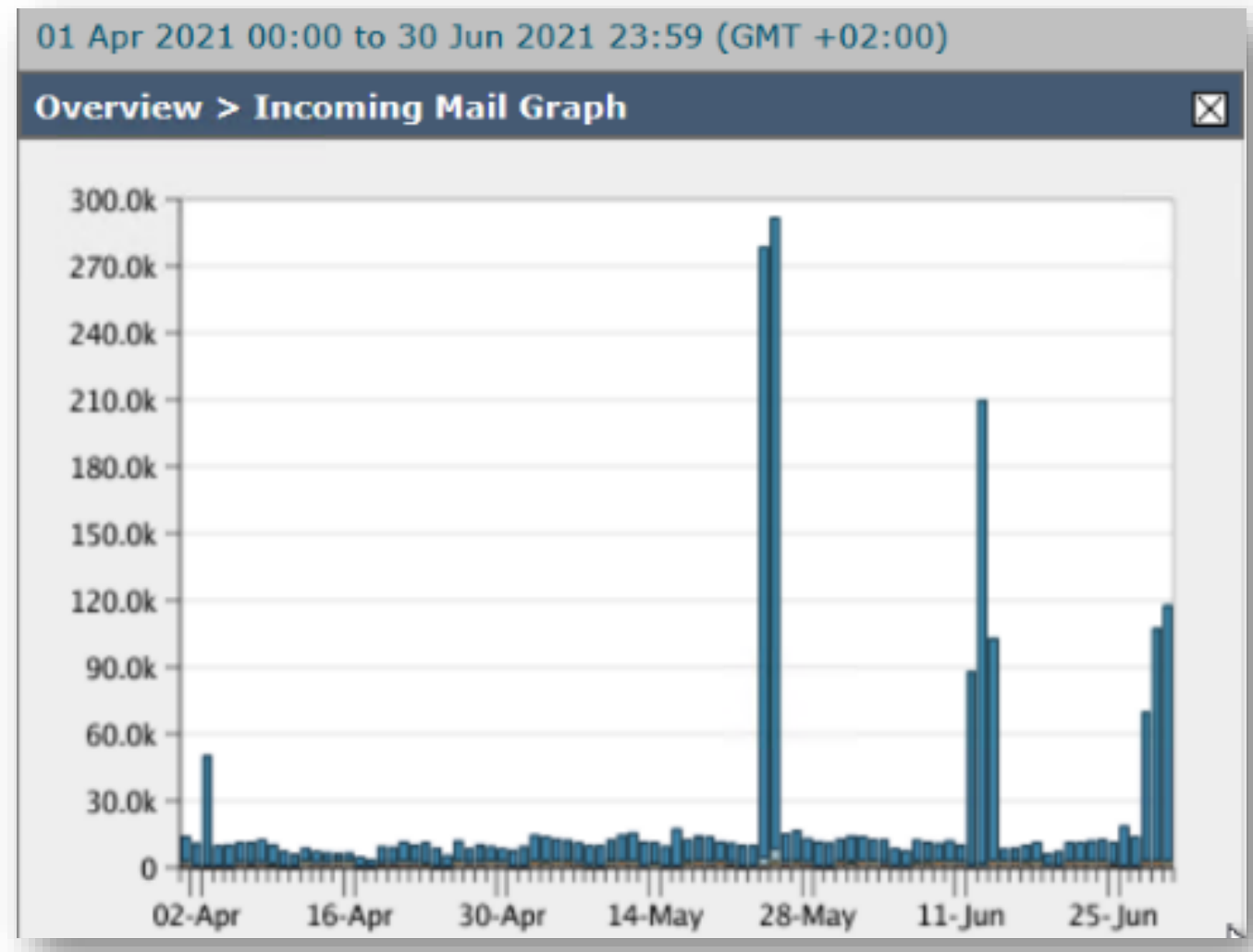
IT-Richtlinien



Passwort

Auswertung E-Mail Spamfilter (Q2 2021: 1. April – 30. Juni 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



Penetration Test Bus

Volvo 7900 A Hybrid Gelenkbus 2. GEN

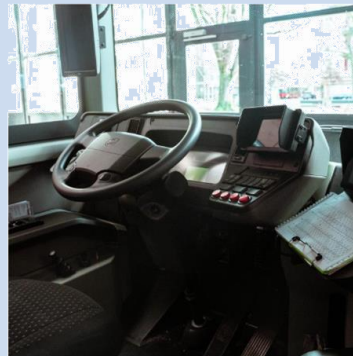
Auf dem Netz von BERNMOBIL verkehren 29 Volvo Gelenk-Hybridbusse



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

Problemstellung

- Extern durchgeführter Penetration Test mittels Blackbox Verfahren sowie gezielten Anwendungsfällen.

Ziel

- Identifizieren von technischen Schwachstellen der Hardware, Software, Schnittstellen, Anwendungen inkl. Fahrzeugtelematik und Netzwerke rund um den vernetzten Bus.

Rahmenbedingungen

- Gleiches Fahrzeug während des gesamten Penetration Tests, kein Mitschnitt der Mobilfunkschnittstelle, nicht destruktiv, Zugriff Telematik System / Volvo Connect vom Hersteller verboten.

Penetration Test Bus - Anwendungsfälle

ITCS-System (Leitsystem)

- Bordrechner
- Bedienterminal am Fahrerplatz
- Bildschirme im Fahrgastraum «Perlschnur»
- Aussenanzeigen (Linie, Ziel)

Werbesystem

- Router
- Bildschirme im Fahrgastraum «Werbung»

Fahrgastzählung

- Messdatensammler
- Türsensoren

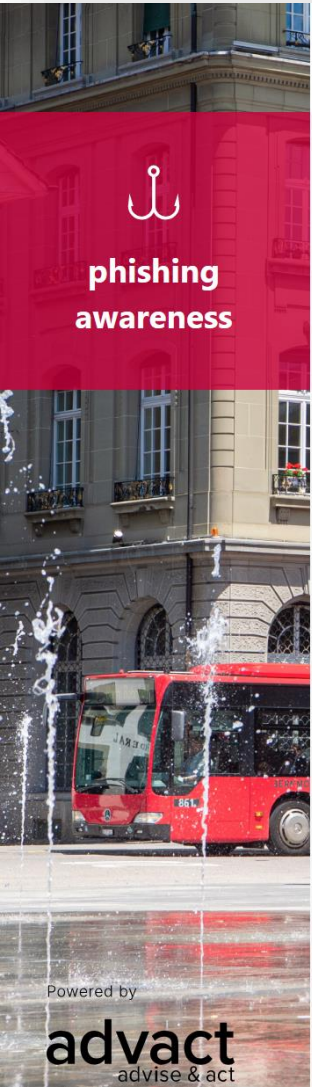
Systeme des Fahrzeugherstellers

- Steuerungen für Fahrzeug Komponenten (Motor, Türen, CAN-Bus etc.)
- Telematik System

Penetration Test Bus - Ergebnisse

Schwachstelle	Verantwortl. Organisation			Gefährdete Systeme			Prio
	BERNIMOBIL	Trapeze	APG	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 - (SMTP) 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



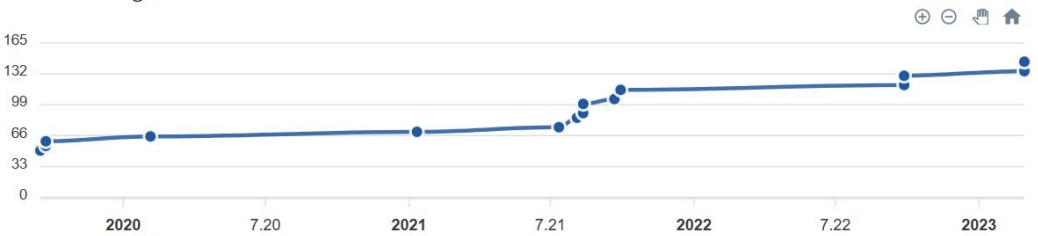
BERNMOBIL
ZUSAMMEN UNTERWEGS

Logout

Ihre persönliche Statistik



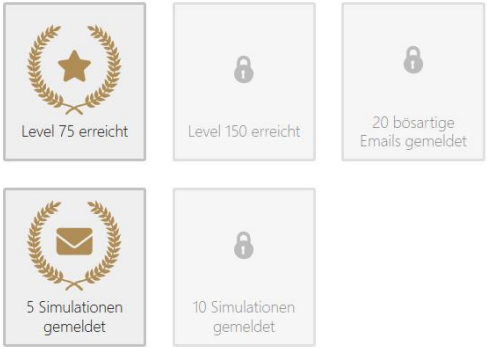
Ihre Leistung



Ihr Fortschritt



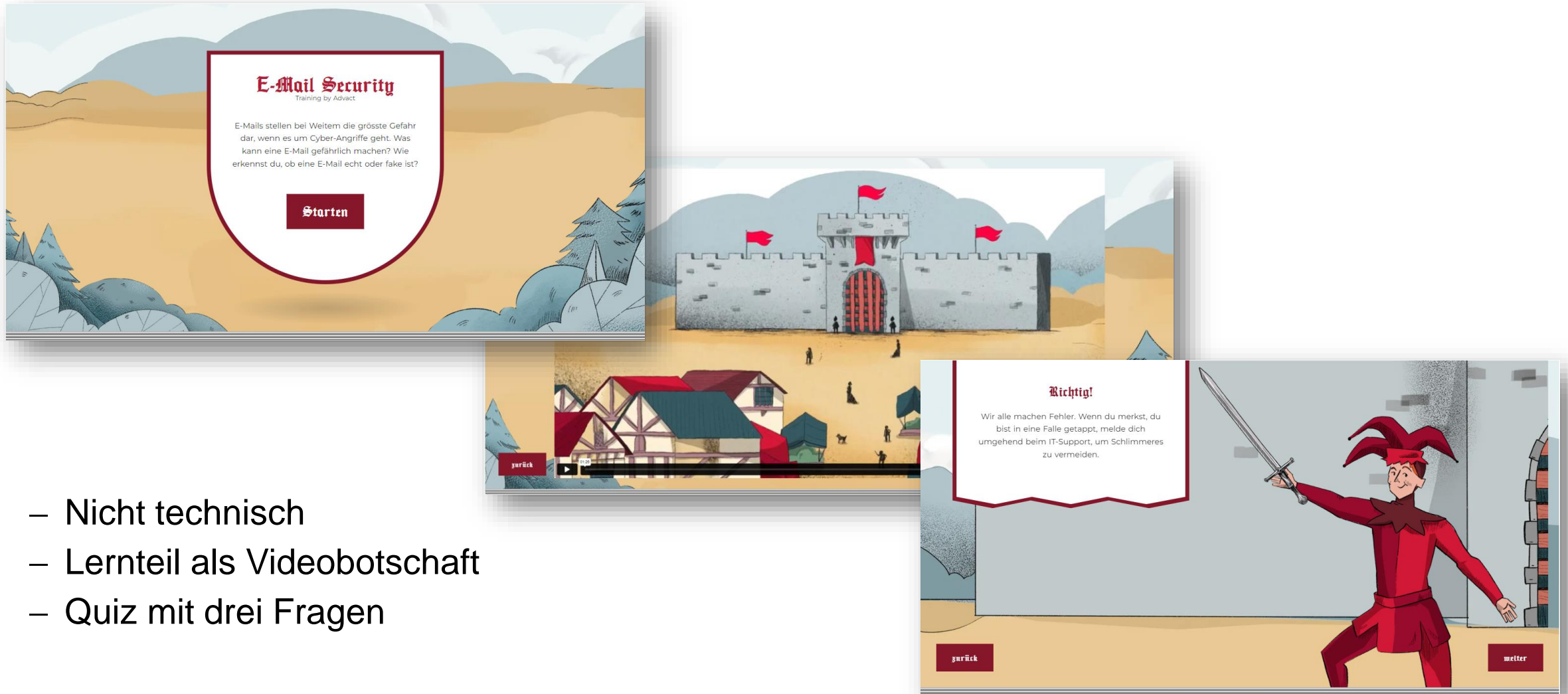
Ihre Erfolge



Rangliste



Phishing Lernmodul



- Nicht technisch
- Lernteil als Videobotschaft
- Quiz mit drei Fragen

Was tun wir sonst noch?

IT-Risikoanalyse

- Alle 3 Jahre vollständige IT-Risikoanalyse
- Jährliche Überprüfung

NCSC/BACS – Geschlossener Kundenkreis

- Zugriff auf den Cyber Security Hub
- Informationen für eigene Organisation
- Alarmierung, wenn eine Meldung vorliegt
- Angebot von Dienstleistungen (GovCERT.ch)

ISMS-Board

- Initiierung
- Basismassnahmen
- Monitoring & Control

Krisenstab

- Cybersicherheit
- Slow Motion Übung

Fazit

- Cyber-Sicherheit beschäftigt uns stark und wird uns weiterhin beschäftigen
- Cyberangriffe sind keine Fiktion, sondern Realität
- Um Cybergefahren zu entgegnen, benötigt es technische sowie organisatorische Massnahmen
- Der Mensch ist der grösste Risiko- und zugleich der grösste Schutzfaktor

Wir verstehen Informationssicherheit nicht als Zustand, sondern als Prozess,
denn eine 100-prozentige Informationssicherheit gibt es nicht.

Cybersicherheit in öffentlichen Verkehrsbetrieben ist entscheidend für den Schutz kritischer
Infrastrukturen und die Gewährleistung eines sicheren und zuverlässigen Betriebs.

