OF-PRO INTELLIGENCE

ofpro-intelligence.eu

DIGITAL EXPOSURE AUDIT

FULL AUDIT — CLEARWEB + DARK WEB

SAMPLE REPORT — FOR ILLUSTRATION PURPOSES ONLY

PRINCIPAL	Thomas B.
FUNCTION	Chief Executive Officer — Company X
SCOPE	Full Audit — Clearweb + Dark Web
JURISDICTION	EU / GDPR
REPORT DATE	10 May 2026
ANALYST	OF-PRO Intelligence EOOD
CLASSIFICATION	**CONFIDENTIAL — PRINCIPAL EYES ONLY**

This report is a sample document produced for demonstration purposes.
All persons, companies, addresses, and data are entirely fictional.

■ LAYER 1 — EXECUTIVE SUMMARY

Written for you — no technical background required. Read this first.

BLUF — Bottom Line Up Front

Thomas B., CEO of Company X, has a HIGH overall digital risk. Three things need to change this week: your passwords, your Strava account, and your wife's Instagram settings. If nothing changes, the most likely attack is a convincing fake email designed to steal money or access. The most dangerous risk is someone showing up at your front door — because they already know your address, your daily route, and when your family is home.

Top Findings

#	WHAT WE FOUND	RISK LEVEL
01	Your passwords from an old data breach are recoverable. If you still use the same password — or a similar one — an attacker can get in.	CRITICAL
02	Your home address is publicly listed in the Dutch property registry. A street-level photo shows no fence, no cameras, and your car on the driveway.	HIGH
03	Your running app (Strava) is public. Your exact morning route, your departure time, and two sections with no cameras are fully visible to anyone.	HIGH
04	Your wife's Instagram account is public and shows your home, your daughter's school activities, and your family schedule.	HIGH
05	Your full profile — photo, mobile number, home address — is listed on four data broker websites. Anyone can find it in three searches.	MEDIUM

What You Need to Do in the Next 48 Hours

1. Change all passwords on your personal email and any account connected to it. Use a unique password for each account — at least 20 characters. Never reuse passwords.
2. Turn your Strava account to private. Turn off route sharing and activity history. This closes the most dangerous physical risk immediately.
3. Ask your wife to turn off location tagging on Instagram today. Go through recent posts together and remove any that show where you live or where your daughter goes to school.
4. Remove your mobile number from your LinkedIn profile. Set your LinkedIn messages to connections only.
5. Brief your assistant (L. de V.): she should never confirm your schedule, location, or travel plans to someone she does not personally recognise.

MLCOA — Most Likely Attack

Fake email attack (spear phishing). An attacker uses everything they know about you — your board memberships, your upcoming conference schedule, your assistant's name — to send a convincing fake email. The goal: get you to click a link that steals your login, or approve a payment that goes to the wrong account. **Likelihood: HIGH. Confidence: HIGH.**

MDCOA — Most Dangerous Attack

Physical approach using your running route. Someone uses your Strava data and home address to identify where and when you are alone, on a predictable route, in a section with no cameras. The same data also allows someone to approach your family at home while you are away. **Likelihood: LOW in isolation — but HIGH if there is a financial or business motive. Confidence: MODERATE.**

■ LAYER 2 — ANALYTICAL REPORT

Scope & Methodology

PARAMETER	DETAIL
Engagement Type	Full Audit — Clearweb + Dark Web
Principal	Thomas B. — CEO, Company X
Jurisdiction	EU / GDPR — Netherlands
Collection Period	07–10 May 2026
Tools Used	theHarvester · SpiderFoot (Human Name scan) · Recon-ng · Maltego CE · Sherlock · Blackbird · Maigret · Holehe · GHunt v2 · HIBP · IntelX · Ahmia (Tor) · ExifTool · Wayback Machine · urlscan.io · VirusTotal · Kadaster · OpenSanctions · Hunter.io
Limitations	Dark web monitoring is point-in-time. Data broker sites may re-populate within 30–90 days without active monitoring. IntelX full dataset requires subscription — content volume documented as intelligence gap.

All collection was performed using publicly accessible sources only. No authentication-gated systems were accessed. No pretexting or social engineering was used. This engagement operates in full compliance with GDPR data minimisation principles (AVG art. 6.1.f) and OF-PRO Intelligence methodology.

Exposure Findings

01 — PII (PERSONALLY IDENTIFIABLE INFORMATION)

Full name, date of birth ([date of birth]), mobile number (+31 6 XXXXXXXX), personal email ([personal email]), and home address ([residential address, Wassenaar]) all confirmed via open sources. Name variations 'T. van den Berg' and 'Thomas vd Berg' are also active across platforms — creating namesake confusion that could be exploited to misdirect security monitoring.

Confidence: HIGH | NATO Admiralty: B-2 | Source: [S1][S2][S3]

02 — DATA BROKER PRESENCE

Principal profile confirmed on 4 aggregator platforms: Oozo.nl (NL), Societe.com (EU), and two international equivalents. Each profile contains photo, mobile number, home address, and partial associate list (spouse name confirmed on 3 of 4). No opt-out requests have been submitted. Data is actively indexed and retrievable within a standard web search.

Confidence: HIGH | NATO Admiralty: A-1 | Source: [S4][S5][S6][S7]

03 — RESIDENCE & PROPERTY

Home address confirmed via Dutch Kadaster public property registry. Property (detached villa, est. value €1.2M) registered in principal's name since 2017. Street-level imagery shows: no perimeter fencing, no visible CCTV, open driveway with premium vehicle visible, letterbox with name label. Neighbourhood (Wassenaar residential) has low foot traffic and limited natural surveillance. Combined with home address exposure on broker sites, this represents a direct physical targeting vector.

Confidence: HIGH | NATO Admiralty: A-1 | Source: [S8][S9]

04 — FAMILY & HOUSEHOLD

Spouse Anna B. operates a public Instagram account (@anna.b****, 1,240 followers). Account contains: vacation destination posts with location tags active, photographs of the home exterior, references to daughter's school activities, and posting patterns that allow inference of household schedule. Daughter (minor, 16) operates a public TikTok account. School uniform is visible in multiple posts — institution identifiable. Family social media presence is the highest-risk family exposure vector and requires immediate action.

Confidence: HIGH | NATO Admiralty: A-1 | Source: [S10][S11]

05 — TRAVEL & PATTERN-OF-LIFE

Strava account ('T.B.') linked to full name via standard web search. Account is public. Morning running route fully mapped: 6.2 km loop departing [street], proceeding via [street 1], [street 2], and returning via [street 3]. Departure window: 06:45–07:10 based on 47 logged runs over 6 months. Two segments of the route pass through low-surveillance wooded paths with no camera coverage. Conference attendance inferrable from LinkedIn posts: 3 confirmed upcoming events with dates and cities.

Confidence: HIGH | NATO Admiralty: A-1 | Source: [S12][S13]

06 — SOCIAL MEDIA

LinkedIn (public profile): 2,847 connections, direct messaging open to all users. Profile lists full employment history, 3 current board memberships, university education ([university]), mobile number in contact section, and links to company website. X/Twitter (@[username]): 890 followers, political opinions expressed, personal frustrations about travel delays and work stress visible — useful social engineering entry points. Instagram: not directly linked to principal but inferrable via spouse's account tags.

Confidence: HIGH | NATO Admiralty: A-1 | Source: [S14][S15]

07 — PROFESSIONAL & CORPORATE

Company X website lists Thomas B. as CEO with photo, direct email ([corporate email]), and mobile. Executive assistant L. de V. is named with her direct email and phone. Org chart structure is partially visible. 3 additional board memberships expose Thomas to intelligence collected on those organisations. Conference speaker history: 5 events publicly listed with dates — historical pattern-of-life data.

Confidence: HIGH | NATO Admiralty: A-1 | Source: [S16][S17]

08 — DARK WEB & BREACH DATA

[personal email] confirmed in 3 separate data breaches via Have I Been Pwned and IntelX: (1) LinkedIn breach 2021 — name, email, employer, phone number exposed; (2) Adobe breach 2013 — email and encrypted password exposed; (3) Gravatar breach 2020 — email and profile hash exposed. Corporate email [corporate email] found in a large aggregated breach dataset (est. 2019). The encrypted password from the 2013 Adobe breach uses an outdated format that can be reversed using freely available tools — enabling account access if the password has not been changed or follows a predictable pattern. Password reuse across accounts is assessed as LIKELY based on the age of the breach and the absence of subsequent security incidents. No active dark web marketplace listings or threat actor discussions identified at time of collection.

Confidence: HIGH (breach data) / **MODERATE** (password pattern) | NATO Admiralty: B-2 | Source: [S18][S19][S20]

10 — SOCIAL ENGINEERING VECTORS

Primary attack surfaces identified: (1) LinkedIn direct message — open to all users, no prior connection required; (2) Executive assistant L. de V. — publicly named and directly reachable, represents a high-value target for someone pretending to be a known contact in order to extract the principal's schedule or trigger a credential reset; (3) Company X generic email (info@[company domain]) — likely monitored by multiple staff, reducing individual vigilance; (4) Conference context — Thomas is a known speaker, making conference-related pretexts highly credible. Company X's email domain lacks full anti-spoofing configuration — meaning fake emails appearing to come from @[company domain] are not blocked at the technical level.

Confidence: HIGH | NATO Admiralty: A-1 | Source: [S16][S21]

12 — HOME & PERSONAL CYBER

Home internet provider range (Wassenaar residential) identifiable via public infrastructure scanning. No VPN usage detected across observed activity. Smart doorbell brand (Ring) inferrable from an Instagram post showing the front door. Ring devices have a documented history of security vulnerabilities — patch status unknown. No evidence of home network security measures. Personal devices are likely unmanaged.

Confidence: MODERATE | NATO Admiralty: C-3 | Source: [S22][S23]

Attack Chain

The identified exposures combine to enable the following adversary action sequence.

Phase 1 — Reconnaissance — An adversary uses LinkedIn, the Company X website, and data broker profiles to construct a complete target profile in under 60 minutes. Home address, mobile number, assistant's name, board memberships, and upcoming conference schedule are all publicly available.

Phase 2 — Credential Access — The encrypted password from the 2013 Adobe breach is reversed using freely available tools. The recovered password is tested against email accounts and the corporate VPN — particularly if a predictable pattern (such as a name combined with a year) is identified.

Phase 3 — Spear Phishing — Using knowledge of The principal's board memberships, upcoming conference schedule, and assistant's name, an adversary crafts a convincing fake email — impersonating a known board contact or conference organiser — and delivers a link designed to steal login credentials or a fake invoice for approval.

Phase 4 — Impact — A compromised corporate email account is used to authorise a fraudulent financial transfer (Business Email Compromise) or to move laterally within Company X's network. In parallel: Strava data and the home address enable surveillance of the morning running route, creating an interception opportunity that requires no digital access whatsoever.

Risk Matrix

EXPOSURE	LIKELIHOOD (1–5)	IMPACT (1–5)	RISK SCORE	AFTER ACTION	PRIORITY
Credential compromise via breach	4	5	20	6 (after password reset + MFA)	CRITICAL
Physical approach via Strava/address	3	5	15	8 (after Strava private)	CRITICAL
Family targeting via social media	3	5	15	6 (after privacy settings)	HIGH
Fake email via LinkedIn/assistant	4	4	16	8 (after awareness brief)	HIGH
Data broker aggregation	5	3	15	4 (after opt-out + monitoring)	HIGH
Home network/IoT exposure	3	3	9	4 (after VPN + patch)	MEDIUM
Email anti-spoofing gap ([company domain])	3	4	12	3 (after configuration)	HIGH

Recommendations

24–48 Hours — Principal Action

- Reset all passwords associated with [personal email] and [corporate email]. Use unique passwords of 20+ characters. Enable two-factor authentication (authenticator app — not SMS) on all accounts.
- Set Strava to private. Disable segment sharing and activity history. Remove existing public run data.
- Brief spouse: disable Instagram location tagging immediately. Review and remove existing posts that show the home or family schedule.
- Remove mobile number from LinkedIn public profile. Set messaging to connections only.

30 Days — Analyst / Vendor Action

- Submit opt-out requests to all 4 identified data broker platforms. Engage an automated removal service for ongoing suppression.
- Brief executive assistant L. de V. on social engineering risks. Establish a verbal confirmation protocol for schedule and travel requests from unknown contacts.
- Audit Company X's email domain anti-spoofing configuration. Enforce full protection to prevent fake emails appearing to come from @[company domain].

- Implement dark web credential monitoring on both email addresses with automated alerting.
- Review Company X website: remove direct mobile number and consider removing the assistant's direct contact from the public page.

90 Days — Structural Hardening

- Install perimeter security measures at residence (CCTV, access control). Consult a physical security specialist.
- Implement hardware security keys (FIDO2) for all corporate and critical personal accounts.
- Commission an annual digital exposure audit. Broker sites re-populate; the threat landscape changes.
- Develop a family digital security protocol: regular privacy briefings for spouse and daughter, agreed social media rules, emergency contact procedure.

Continuous — Monitoring Requirements

- Google Alerts on name variants: 'Thomas B.', 'T. van den Berg', 'T.B.'.
- Dark web credential monitoring — both email addresses — with real-time alerting.
- Annual review of data broker presence and opt-out status.
- Quarterly review of social media privacy settings across all family accounts.

Alternative Hypotheses

H1 — Opportunistic, Not Targeted (LIKELY — Confidence: MODERATE)

The identified exposures are the result of routine data broker aggregation and historical breaches that affect millions of individuals. No specific adversary has Thomas B. as a deliberate target. Risk is elevated by exposure volume, but there is no evidence of active adversarial collection. Action is still warranted — opportunistic actors also exploit these vectors.

Confirmation: Absence of any dark web discussion, forum mention, or targeted phishing attempt post-credential monitoring activation.

Elimination: Identification of targeted surveillance indicators — repeated queries on the principal's name, or direct contact attempts using personal data not publicly obvious.

H2 — Insider Threat or Business Dispute (UNLIKELY — Confidence: LOW)

A current or former employee, business partner, or competitor is actively conducting OSINT on the principal as part of a corporate intelligence or defamation campaign. The public exposure would facilitate this. No supporting indicators identified at this time.

Confirmation: Evidence of structured data collection on the principal from a traceable source; receipt of targeted communications referencing non-public personal details.

Elimination: No structured collection pattern identified after 90 days of monitoring.

Deception Audit

Stale data risk — Breach data (particularly from 2013) is over a decade old. The password may have been changed. The technical reversibility of the encrypted password remains a valid risk but may not reflect current credentials. Confidence in live credential access downgraded from HIGH to MODERATE.

Selection bias — Collection was conducted over a four-day window. Broker sites may have updated or removed data since collection. Findings represent a point-in-time snapshot, not a continuous intelligence picture.

Namesake risk — Name variants 'T. van den Berg' and 'Thomas vd Berg' create potential for false attribution. All findings verified against at least two corroborating identifiers before inclusion. Single-source findings marked UNCONFIRMED.

Sources

REF	SOURCE	TYPE	DATE	NATO RELIABILITY	NATO CREDIBILITY
S1	Kadaster.nl — property	Official public	07 May	A — Reliable	1 — Confirmed

REF	SOURCE	TYPE	DATE	NATO RELIABILITY	NATO CREDIBILITY
	registry	record	2026		
S2	Oozo.nl — principal profile	Data aggregator (NL)	07 May 2026	B — Usually reliable	2 — Probably true
S3	LinkedIn.com — principal profile	Social/professional platform	07 May 2026	A — Reliable	1 — Confirmed
S4–S7	Oozo.nl, Societe.com + 2 international aggregators	Data aggregators (4x)	08 May 2026	B — Usually reliable	2 — Probably true
S8	Kadaster.nl — property record	Official public record	07 May 2026	A — Reliable	1 — Confirmed
S9	Google Maps Street View	Geospatial imagery	07 May 2026	B — Usually reliable	2 — Probably true
S10–S11	Instagram @anna.b****, TikTok (minor)	Social media — public	08 May 2026	A — Reliable	1 — Confirmed
S12	Strava — T.B. — public profile	Fitness platform	08 May 2026	A — Reliable	1 — Confirmed
S13	LinkedIn — conference listings	Professional platform	08 May 2026	A — Reliable	1 — Confirmed
S14–S15	LinkedIn, X/Twitter — principal profiles	Social media — public	08 May 2026	A — Reliable	1 — Confirmed
S16–S17	[company domain] — company website	Corporate website	09 May 2026	A — Reliable	1 — Confirmed
S18	HaveIBeenPwned.com	Breach notification service	09 May 2026	A — Reliable	1 — Confirmed
S19–S20	IntelX — breach datasets	Dark web / breach intelligence	09 May 2026	B — Usually reliable	2 — Probably true
S21	MXToolbox — DNS check [company domain]	Technical infrastructure	09 May 2026	A — Reliable	1 — Confirmed
S22–S23	Shodan.io — ISP range, Instagram post	Technical / social media	09 May 2026	C — Fairly reliable	3 — Possibly true

Intelligence Gaps

GAP	IMPACT IF UNRESOLVED	PRIORITY COLLECTION STEP
Whether the recovered password is in active use	Credential compromise may already be in progress	Test against known account recovery flows in a controlled environment
Current security posture of home network	Home device attack surface unquantified	Active ISP range scan (Shodan) + smart doorbell firmware version check
Whether daughter's TikTok account has disclosed school name explicitly	Minor's safety risk elevated if school is identifiable	Manual review of account content — last 90 days
Anti-spoofing enforcement status at supplier/client domains	Spoofed supplier emails may reach principal without flagging	DNS check of top 5 Company X suppliers
Whether any dark web forum has discussed the principal since collection	Active targeting may have begun	Continuous dark web monitoring — 90-day window
IntelX full breach dataset content	Full credential exposure scope unknown	Documented as gap — full access requires subscription