fieldfisher NKF Data-Sec

DACH Cybersecurity Summit

Intro

Cyber-Attacken

- Im vergangenen Jahr waren **72 Prozent der Unternehmen in der DACH-Region von Ransomware** betroffen. *(IDC Studie „Cybersecurity in DACH 2022“)*
- **81% der Unternehmen in der DACH Region sahen sich erfolgreichen Email-basierter Angriffen ausgesetzt** im vergangen Jahr. *(Barracuda - Market Report „2023 email security trends“)*
- Die **Schadenssumme durch Cyberangriffe belief sich im vergangenen Jahr auf rund 203 Milliarden Euro** allein in Deutschland. *(Bitkom)*
- Im Schnitt dauert es **22 Stunden bis eine Sicherheitsattacke erkannt** und **weitere 44 Stunden bis darauf reagiert und der Angriff behoben wird**. Dabei werden durchschnittlich **9 verdächtige Emails pro Tag bei IT Abteilungen** gemeldet. *(Barracuda – Market report „2023 spear-phishing trends“)*
- **Ransomware/Phishing-Emails, DDoS Attacken und die Nutzung unautorisierter Devices (USB-Sticks, private Geräte) an Unternehmensnetzwerken gelten als wahrscheinlichste Einfallstore** für Cyber-Angriffe. *(Lünendonk-Studie 2023 „Von Cyber Security zu Cyber Resilience“)*

Allgemeine Organisations- und Sorgfaltspflichten der Geschäftsleitung

- Bereitstellung der finanziellen Mittel und technisch-organisatorischen Ressourcen für IT-Sicherheit
- Sicherstellung angemessener Maßnahmen zur IT-Sicherheit, um das Unternehmen vor Cyberangriffen zu schützen.
- Angemessenes Risikomanagement für Cyberangriffe, einschließlich der Identifizierung von Risiken, der Bewertung ihrer Auswirkungen und der Umsetzung von Maßnahmen zur Risikominderung.
- Im Falle eines Cyberangriffs ist der Geschäftsführer dafür verantwortlich, angemessene Maßnahmen zur Schadensbegrenzung zu ergreifen, um die Auswirkungen des Vorfalls zu minimieren.

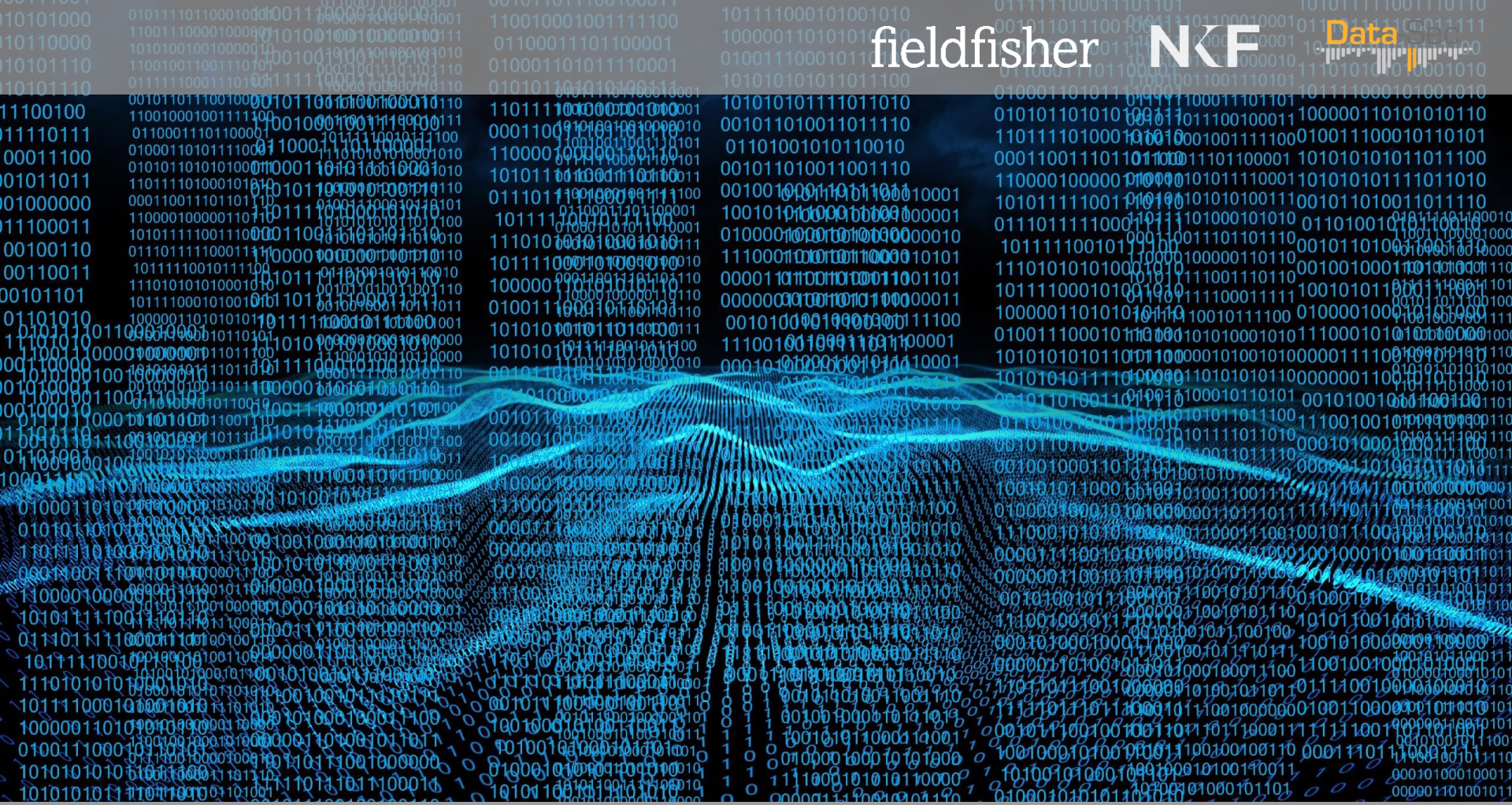
Incident Response Plan

- Klare Definition der Ziele und des Zwecks des IRP
- Definition und Zuweisung von Rollen und Verantwortlichkeiten. Klare Hierarchien und Kommunikationswege.
- Incident-Klassifizierung und Eskalationsverfahren
- Richtlinien zur Dokumentation von Sicherheitsvorfällen, einschließlich aller relevanten Informationen, wie Zeitpunkt, Art des Angriffs, betroffene Systeme und ergriffene Maßnahmen.
- Wiederherstellungspläne
- Kommunikationsstrategie

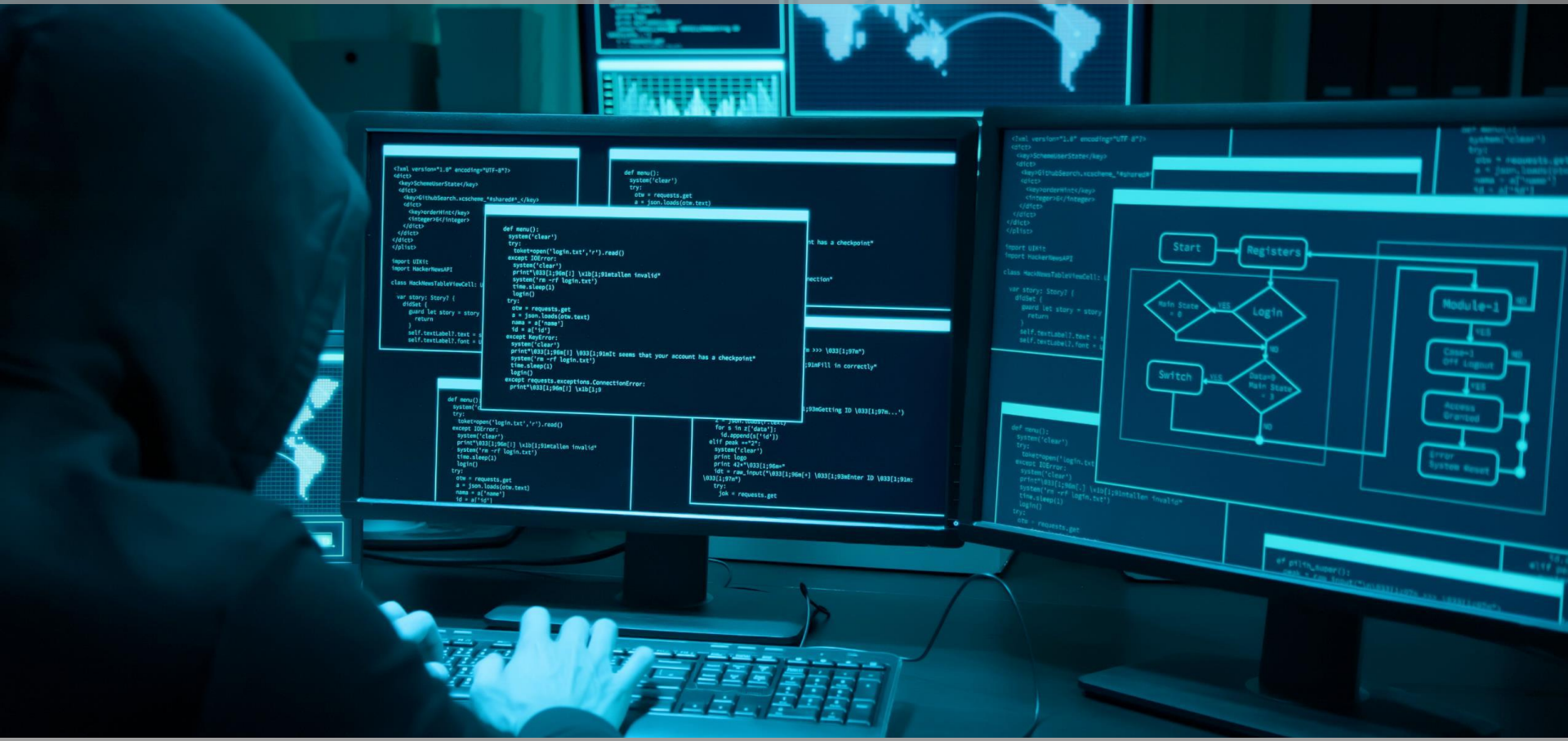
Unser Fall:

Die Trendshop Commerce AG aus Zürich verkauft über ihre Onlineshops sowie im Einzelhandel in Deutschland, Österreich und der Schweiz Geschenkartikel an Verbraucher. Sie hat Mitarbeiter an allen Standorten und insgesamt ca. 400.000 registrierte Kunden und Niederlassungen in Wien und Hamburg, wo sie jeweils eigene Tochtergesellschaften gegründet hat. Am Freitag, 9.9.2023 um 10:38 bemerkt die IT-Abteilung, dass ein Datenbanksystem mit Ransomware infiziert.

Zürich


fieldfisher
NKF
Data

fieldfisher NKF DataSec



Trendshop ruft bei NKF an

fieldfisher NKF Data-Sec

- Was ist genau passiert?
- Welche Server und Daten sind betroffen?
- Wo sind die Standorte der Server?
- Ist der Back-up verschlüsselt?
- Allenfalls ist eine Meldung beim EDÖB notwendig, wenn ein hohes Risiko für die Persönlichkeit oder die Grundrechte betroffenen Personen besteht
- Meldeportal: https://databreach.edoeb.admin.ch/repo

Kanzlei Niederer Kraft Frey, Zürich

Erster Call Anwälte + Data Sec

fieldfisher NKF Data-Sec

Perspektive / ToDos Österreich

fieldfisher NKF Data-Sec

- Art des Vorfalls (Hacking, Ransomware,…)
- Welche Systeme / Datenkategorien sind betroffen? Gibt es funktionierende Backups?
- Umfang des Vorfalls? (Anzahl Betroffene, Länder)
- Gibt es ein Krisenteam? Wer gehört dazu?
- Was ist Dritten über die Situation bekannt?
- Gab es bereits Kontakt mit Datenschutzbehörden oder Strafverfolgungsbehörden?

Zwischenstand forensische Untersuchung und Verhandlung mit den Angreifern

fieldfisher NKF DataSec

Zürich

Perspektive / ToDos Deutschland

- Einbindung des betrieblichen Datenschutzbeauftragten (in DE in der Regel in allen Unternehmen mit + 20 Mitarbeitern verpflichtend)
- Risiko Bußgelder
- Welche lokale Aufsichtsbehörde ist zuständig für Art. 33, 34 DSGVO Meldungen?
- Schrittweise Meldungen gem. Art. 33 Abs. 4 DSGVO
- Risiken überobligatorischer Meldungen: Schadenersatz(massen)klagen in Deutschland
- Art. 34: Auskunftsansprüche antizipieren!
- Strafanzeige? Keep Calm!

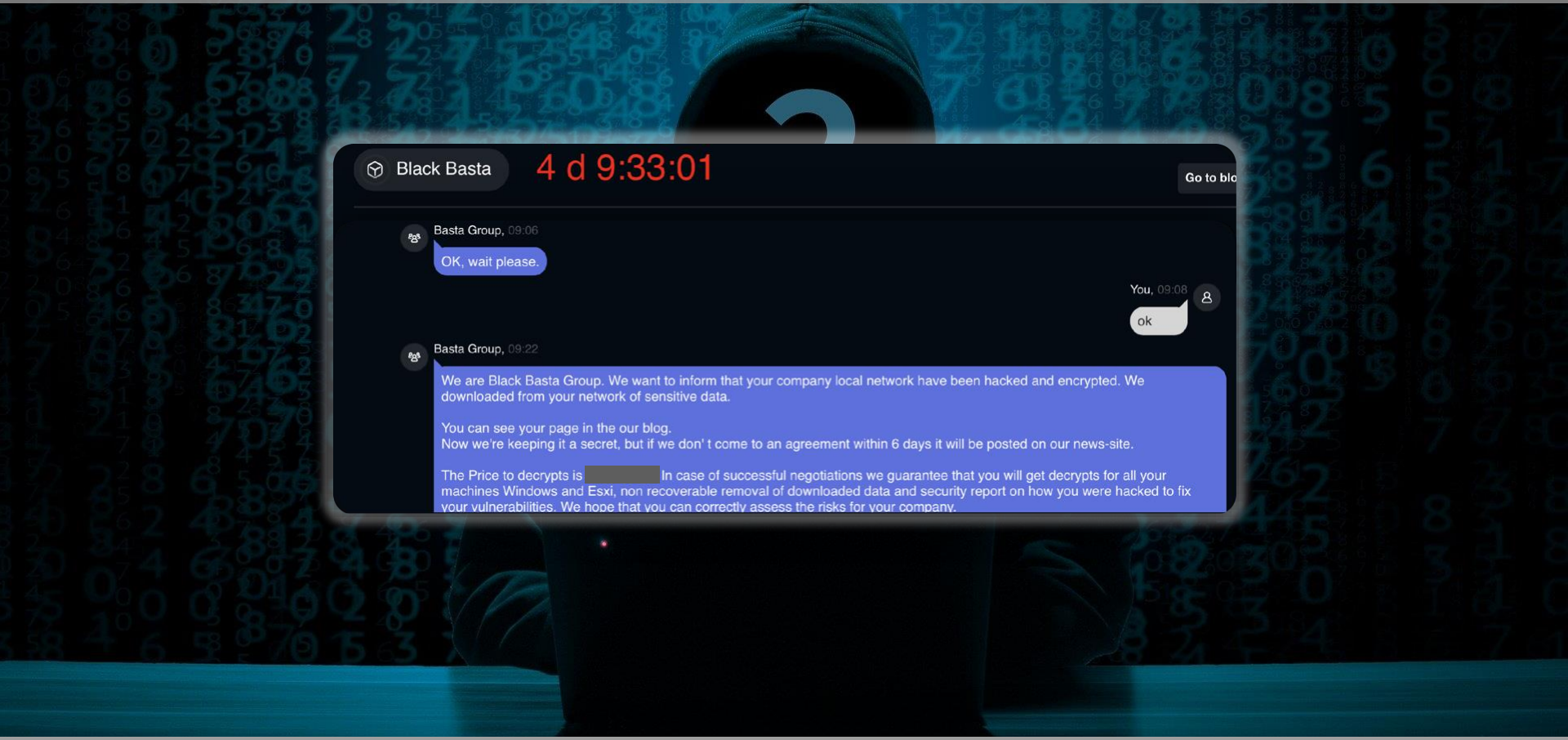
Perspektive / ToDos Schweiz

fieldfisher NKF Data-Sec

- Kontaktaufnahme mit **Cyber Polizei** des Kantons Zürich
- Kontaktaufnahme mit externen **technischen Experten**
- Proaktiv die **Versicherung** kontaktieren. Haben Sie eine Cyber Incident Insurance?
- Möglicherweise **Meldung an EDÖB** – sobald wie möglich
- Strategie re **Lösegeldzahlung** festlegen nach dem Gespräch mit der Cyber Polizei und den technischen Experten
- Datenschutzbehörden CH und EU **Notifikationspflichten**? Schweiz Mitteilung "so bald wie möglich"
- **Vertragliche Pflichten** gegenüber Kunden und Geschäftspartnern?
- Pflicht der **Schadensminimierung**: sollte der Internet/E-Mailverkehr lahmgelegt werden, müssten Kunden und Geschäftspartner informiert werden, um Vertragsverletzungen und finanzielle Schäden zu vermeiden.
- **Kommunikation** gegen Aussen vorbereiten
- Interne Mitteilung an die **Mitarbeiter**
- Interne **Dokumentation/Reglemente**: Data Breach Response Plan; IT Sicherheitsreglemente?
- **Task Force** / Pikettdienst organisieren

Kanzlei, Zürich

Unternehmenszentrale, Zürich


Black Basta
4 d 9:33:01
Go to blo
Basta Group, 09:06
OK, wait please.
You, 09:08
ok
Basta Group, 09:22
We are Black Basta Group. We want to inform that your company local network have been hacked and encrypted. We downloaded from your network of sensitive data.
You can see your page in the our blog.
Now we're keeping it a secret, but if we don' t come to an agreement within 6 days it will be posted on our news-site.
The Price to decrypts is [redacted] In case of successful negotiations we guarantee that you will get decrypts for all your machines Windows and Esxi, non recoverable removal of downloaded data and security report on how you were hacked to fix your vulnerabilities. We hope that you can correctly assess the risks for your company.

fieldfisher NKF Data-Sec

fieldfisher NKF DataSec

Lessons learned und Q & A

fieldfisher NKF DataSec