WIDERSTANDSFÄHIGKEIT IST DIE BESTE VERTEIDIGUNG

LEHREN AUS DEN FEHLERN ANDERER

LINUS NEUMANN

ICH VERSUCHE, KRISEN ZU PROBLEMEN ZU DEGRADIEREN

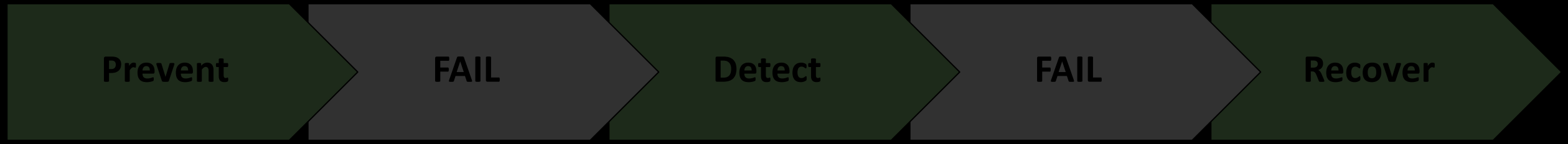
Work

- Red Teaming
- Penetration Testing
- Incident Management
- IT-Security Strategie
- https://srlabs.de

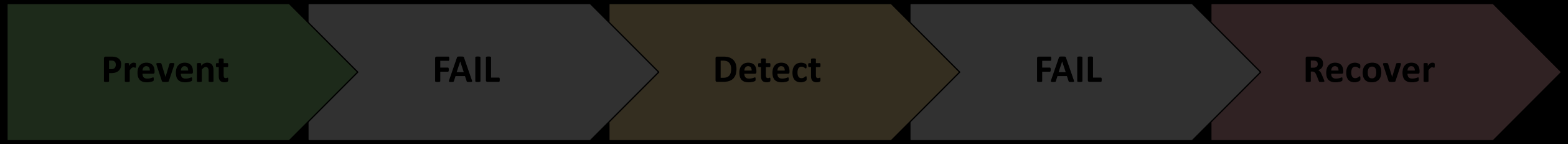
Life

- Wahlsysteme
- Staatstrojaner
- Politik
- Podcast Logbuch:Netzpolitik
- https://logbuch-netzpolitik.de

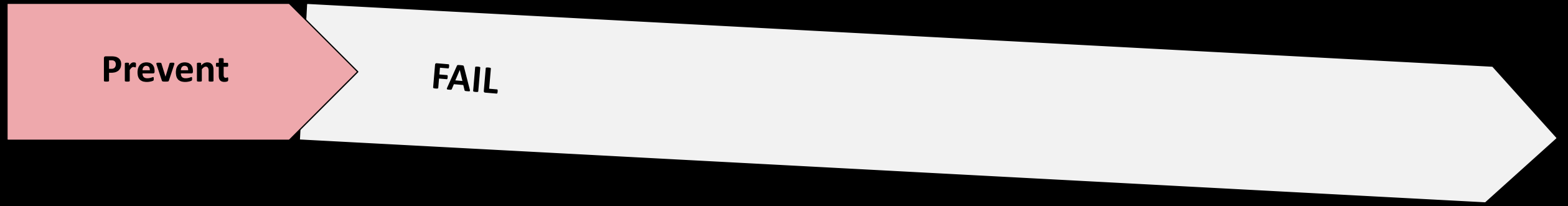
How it should be:



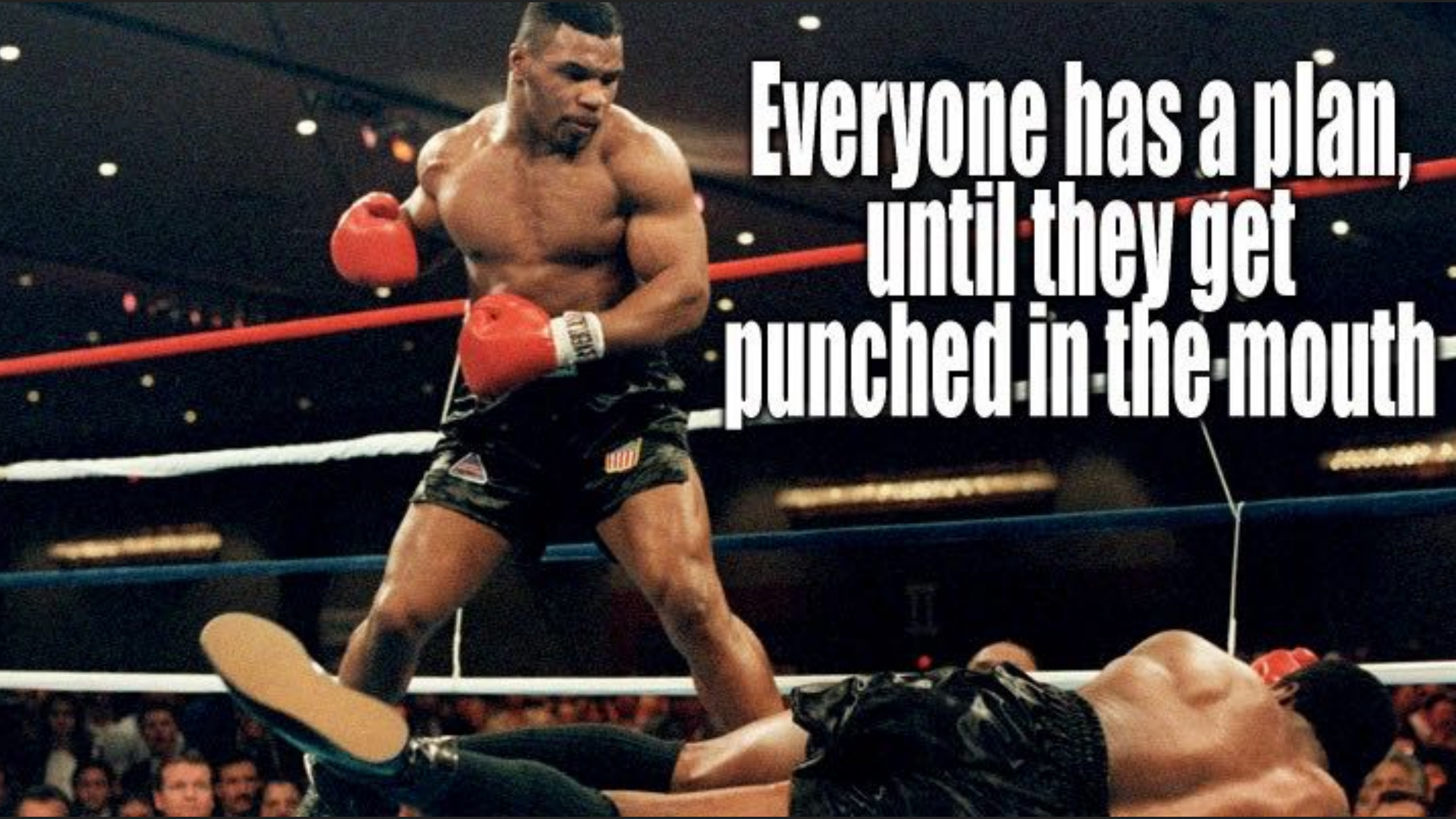
How you think it is:



How it really is:



LINUS NEUMANN


Everyone has a plan,
until they get
punched in the mouth

Kein Backup,
Kein Mitleid!

REALITÄTSPFAD A

Lang und schmerzhaft

Business	IT Security	IT

Wir veröffentlichen in 10 Tagen.
Wir haben einen Decrypter.
Wir wollen 100 Mio.

Junge, beweise doch erstmal, dass du die Dateien hast.

Kein Thema. Hier ist die Liste.
listing.txt
Such dir drei aus, schicken wir dir.

Okay, schick mal X, Y und Z.

Gerne, Bruder.
x.docx y.xlsx z.exe

Die Liste der Dateien gibt es für umme.

LINUS NEUMANN

Wir stellen gerade von Tapes wieder her.

Stell dir mal vor, wenn wir alles releasen!

Na ja, nichts wirklich kritisches dabei.

Wir verkaufen das an die Konkurrenz!

Kannst du gern probieren.

Die Veröffentlichung bringt meist einen nur geringen Schaden (für dich).

Ey, diese Tapes dauern echt lange.
Wir zahlen dir 25Mio.

Wir wollen 100Mio und du hast noch 7 Tage. Danach wird es teurer!

Alter, in 7 Tagen sind wir fertig.
Du kannst mir maximal 50Mio sparen, also zahle ich dir 40.

Wir wollen 70Mio. Letztes Angebot!
Gilt nur 24 Stunden!!!

Je länger das hier dauert,
desto weniger ist der Decrypter wert.

Für die Angreifer geht es um alles oder nichts.

Na gut. 60Mio, weil du es bist!
LETZTE PREIS!

Schade. Das hätte hier eine WIN-WIN-Situation werden können.

Ich red mal mit dem Boss.

Du verhandelst du mit Level 1 Customer Support. Der hat klare Grenzen.

Okay. 50Mio.
Das ist ALLERLETZTE PREIS!

Woher weiß ich, dass du die Dateien überhaupt wieder herstellen kannst?

Schick mir zwei, mein Freund.

Jo. a.encrypted und b.encrypted

Guck mal: a.decrypted und b.decrypted

Vergewissere dich, dass dein Freund die Dienstleistung erbringen kann.

Hier unsere BTC wallet:
bc1qar0srrr7xfkvy5l643lydnw9re59gtzzwf

Ok, wir schicken dir mal einen Satoshi.

Ist angekommen.

Na gut, hier ist der Rest.

Wir haben deine Dateien gelöscht.
Hier ist das deletion.log

Bezahle nur,
wenn du einen Business Case hast!!!
Meistens hast du keinen!

REALITÄTSPFAD B

Problem statt Krise

Business	IT Security	IT

LINUS NEUMANN

IT Security

Business

IT

! **Du brauchst priorisierte Recovery des Business.**
Übliche Backup-Konzepte sind das Gegenteil!

Best practice	Implementation
Immutable	▪ Nur-Schreiben ▪ Manipulationssicher
Independent	▪ Eigene Infrastruktur
Isolated	▪ Eigenes IAM ▪ Enge Zugriffskontrolle
Versioned	▪ Mehrere Versionen ▪ Inkrementell
Verified	▪ Regelmäßige Ende-zu Ende Wiederherstellung
Monitored	▪ Erfolg sichergestellt ▪ Integrität sichergestellt

Best practice	Implementation
Immutable	▪ Nur-Schreiben ▪ Manipulationssicher
Independent	▪ Eigene Infrastruktur
Isolated	▪ Eigenes IAM ▪ Enge Zugriffskontrolle
Versioned	▪ Mehrere Versionen ▪ Inkrementell
Verified	▪ Regelmäßige Ende-zu Ende Wiederherstellung
Monitored	▪ Erfolg sichergestellt ▪ Integrität sichergestellt
Risk-based	▪ Wiederherstellung des Geschäftsbetriebs priorisiert

Du schützt ein Business, nicht eine IT!

EIN WIEDERANLAUF WILL GEPLANT SEIN

Nutzdaten

Geschäftskritisch

Konfiguration

System

Redundant
Statisch
Unkritisch

“NO RANSOM POLICY”

! Das müsst ihr euch erstmal leisten können!

“WIR HABEN ES HINTER UNS”

! Es gibt genug andere Angreifer, die deine Schwachstellen auch ausnutzen.

IT-SICHERHEIT IST KEIN ZUSTAND, SONDERN EIN PROZESS!

Wau Holland

DEFINITION: RESILIENZ

die Fähigkeit, sich **schnell und vollständig** von Unglücksfällen zu erholen

die Fähigkeit, wieder **glücklich und erfolgreich** zu sein, nachdem etwas Schlimmes passiert ist

SICHERHEIT GEHT ÜBER PRÄVENTION HINAUS!

- **Security Lifecycle**

!

Prävention und Detektion gibt es als Service,
Wiederherstellung will trainiert sein.

VERSTEHE, WAS DU SCHÜTZT.
ES IST NICHT DIE IT.

VERSTEHE, WOGEGEN
DU ES SCHÜTZT.