Sichere Infrastruktur: Best Practices zum Schutz Ihrer IT

Präsentiert von:
Manfred Blum und Dennis Paun

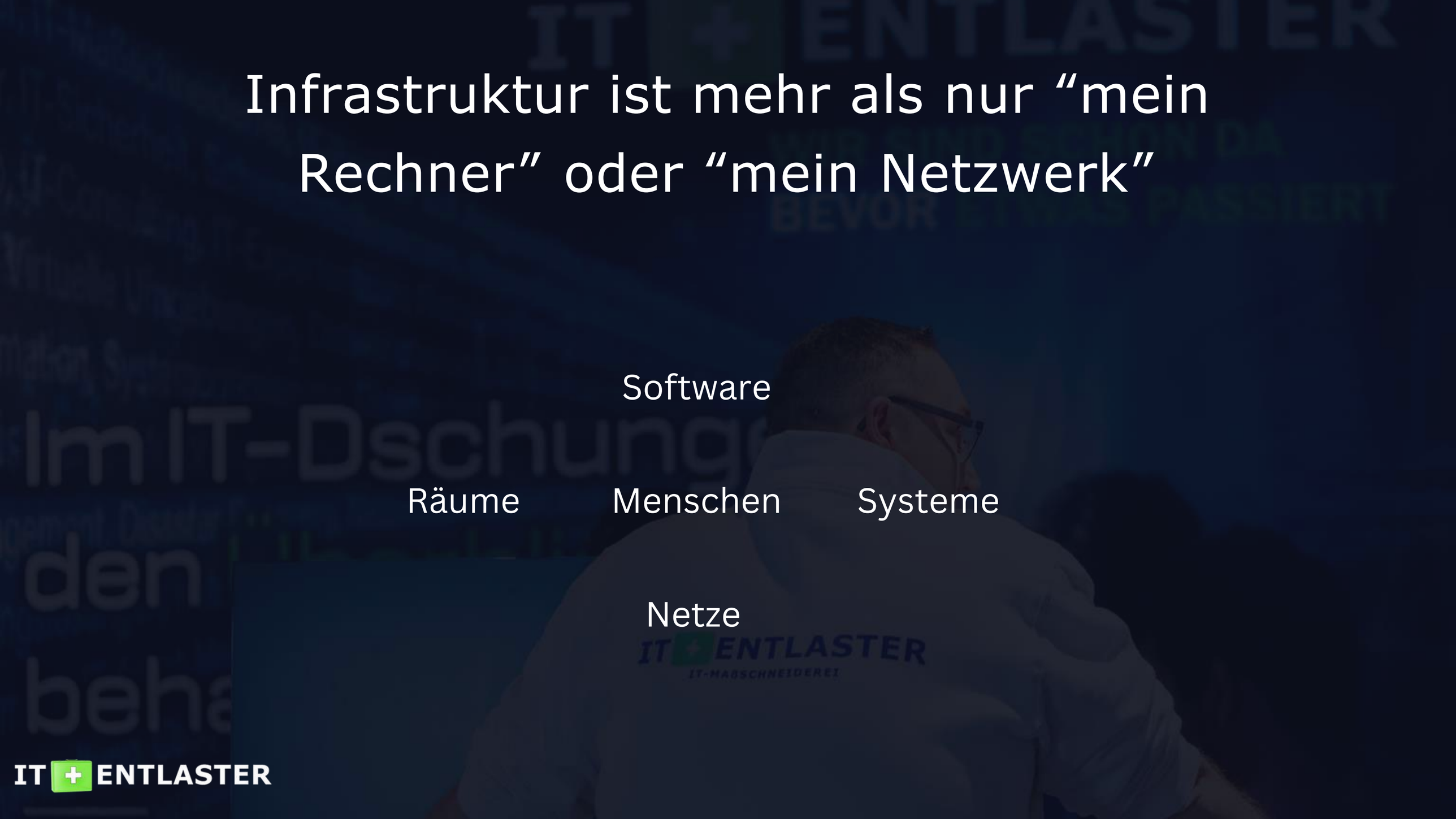
IT ENTLASTER

Infrastruktur ist mehr als nur “mein Rechner” oder “mein Netzwerk”

Software

Räume Menschen Systeme

Netze



Um mal bei IT zu bleiben

Firewall

Regelmässige Updates

Aktiver Support

Regelwerk getreu dem Motto
“So viel wie nötig aber so wenig wie möglich”

Web Veröffentlichungen nur mit WAF

IT ENTLASTER

Um mal bei IT zu bleiben

Switche

gemanaged, regelmässige Updates

aktiver Support

keine Standard Zugangsdaten

IT ENTLASTER

Um mal bei IT zu bleiben

Netzwerksegementierung

getreu dem Motto
“So viel wie nötig aber so wenig wie möglich”

Isolierung unsicherer Systeme
(Drucker, alte Server)

Management Zugriffe

Workstations

Server

Um mal bei IT zu bleiben

WLAN

802.x Computer-Authentifizierung

keine fremden Systeme im internen Netz

Aktuelle WLAN Systeme

WLAN am besten immer extern

Kleine Umgebungen -> WLAN Schlüssel regelmässig ändern

IT ENTLASTER

Um mal bei IT zu bleiben

VPN

Immer 2FA

Keine privaten Geräte

getreu dem Motto
“So viel wie nötig aber so wenig wie möglich”

Aktuelle Software

IT ENTLASTER

Um mal bei IT zu bleiben

Endpoints / PCs

Regelmässige Updates

Aktiver Support

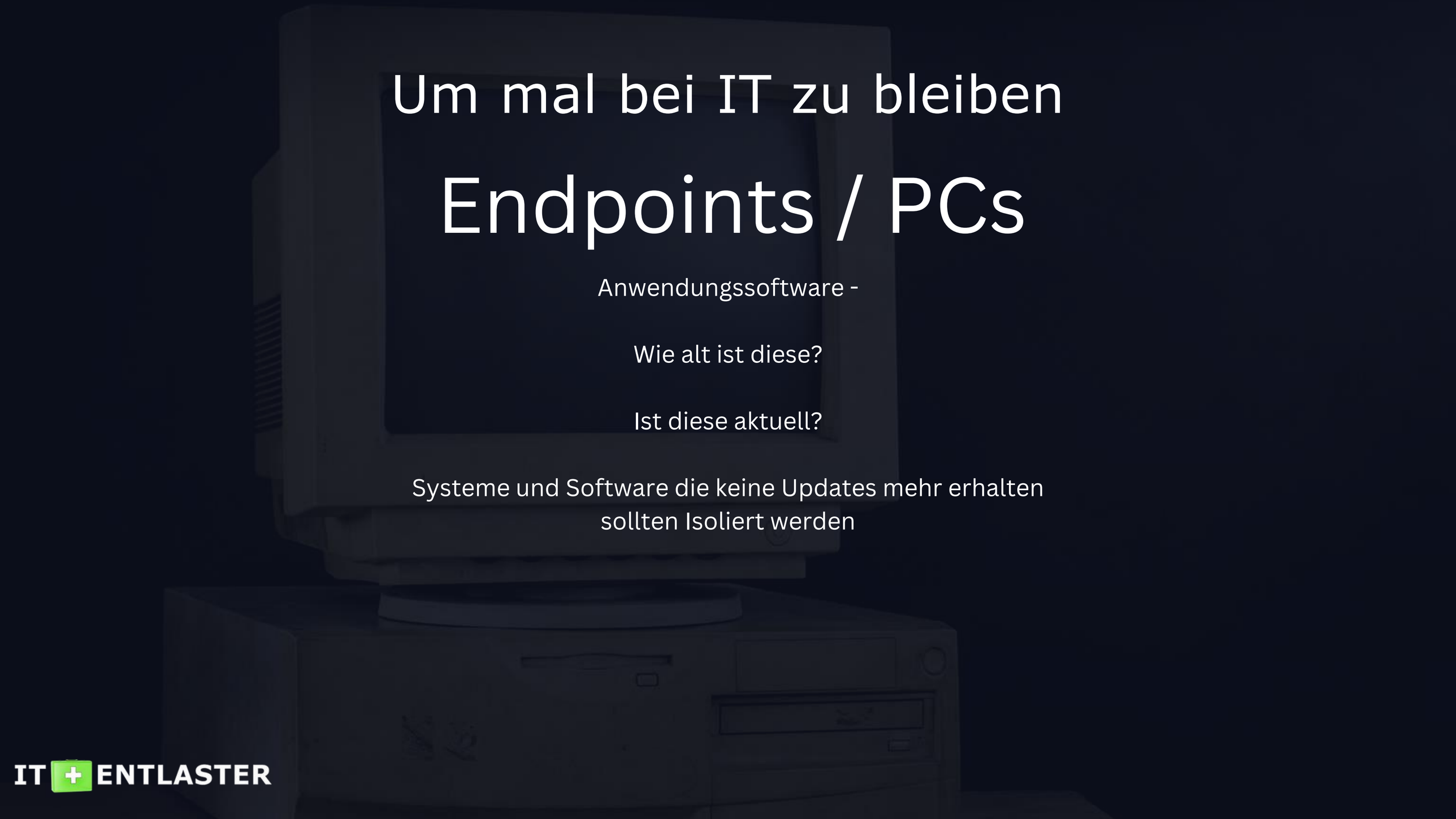
Zugang
(Kennwörter und Physisch)

Ports (USB) sollten eingeschränkt und überwacht werden

Verschlüsselung der Festplatte -> Ein "must have" bei Notebooks

Rechtevergabe
getreu dem Motto
“So viel wie nötig aber so wenig wie möglich”

IT ENTLASTER



Um mal bei IT zu bleiben

Endpoints / PCs

Anwendungssoftware -

Wie alt ist diese?

Ist diese aktuell?

Systeme und Software die keine Updates mehr erhalten sollten Isoliert werden

IT ENTLASTER

Um mal bei IT zu bleiben

Server

Regelmässige Updates

Isolation alter Systeme

Prüfen ob ich denn wirklich jede installierte Software auch brauche

Wie ist die Software installiert?
Berechtigung von Diensten

Um mal bei IT zu bleiben

Authentifizierung

Komplexe Kennwörter mindestens 12 Zeichen

Regelmässige Änderung administrativer Kennwörter
(nicht nur Windows)

Regelmässige Prüfung nach offengelegten Kennwörtern
(z.B. Specops Password Auditor)

IT ENTLASTER

Um mal bei IT zu bleiben

Active Directory

Regelmässiges AD Audit
-> Ping Castle

Einige Punkte dazu sind:
- Domänen-Admins
- Builtin\Administratoren
- Schema-Admins
- KRBTGT-Kennwort
- Protected Users

LAPS
TIER-MODELL

Um mal bei IT zu bleiben

E-Mails

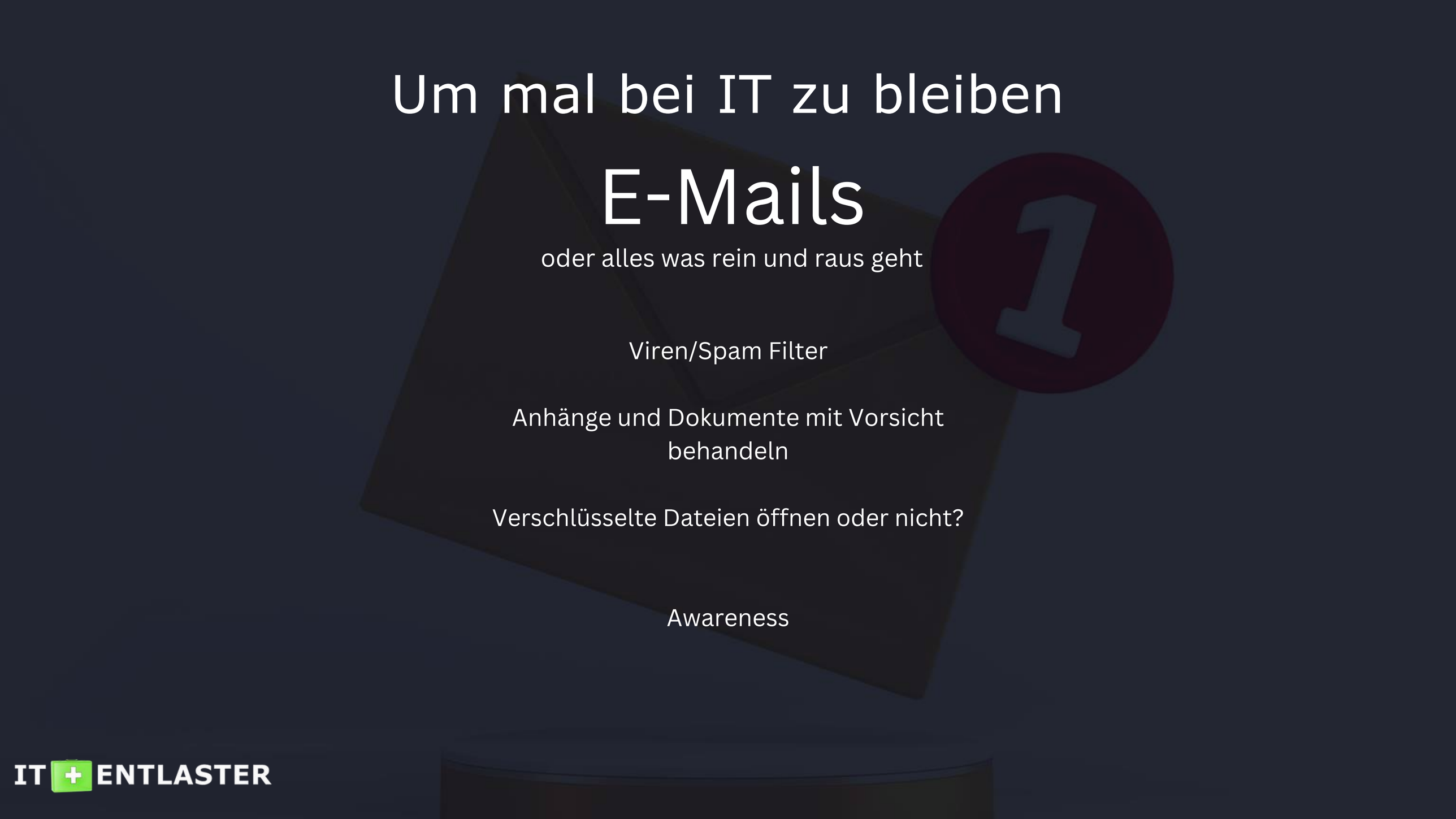
oder alles was rein und raus geht

Viren/Spam Filter

Anhänge und Dokumente mit Vorsicht behandeln

Verschlüsselte Dateien öffnen oder nicht?

Awareness



IT ENTLASTER

Um mal bei IT zu bleiben

Daten

Klassifizierung

Welche Daten habe ich ?

Wo liegen diese?

Kennwörter nicht in Text oder Word Dateien

Nutzung von KeePass oder Passbolt

IT ENTLASTER

Um mal bei IT zu bleiben

Storage

2FA

keine Standardkennwörter

Multiadmin bei gravierende Änderungen

unlöschbare Snapshots

aktuelle Software

Um mal bei IT zu bleiben

Backup

Offsite

Offline

Cloud

Kontrolle

Recovery Tests

Um mal bei IT zu bleiben

Logs -> Kein Holz (eng.)

DNS

DHCP

Windows Systeme

Firewall

Switche

Linux

SIEM -> Enginsight

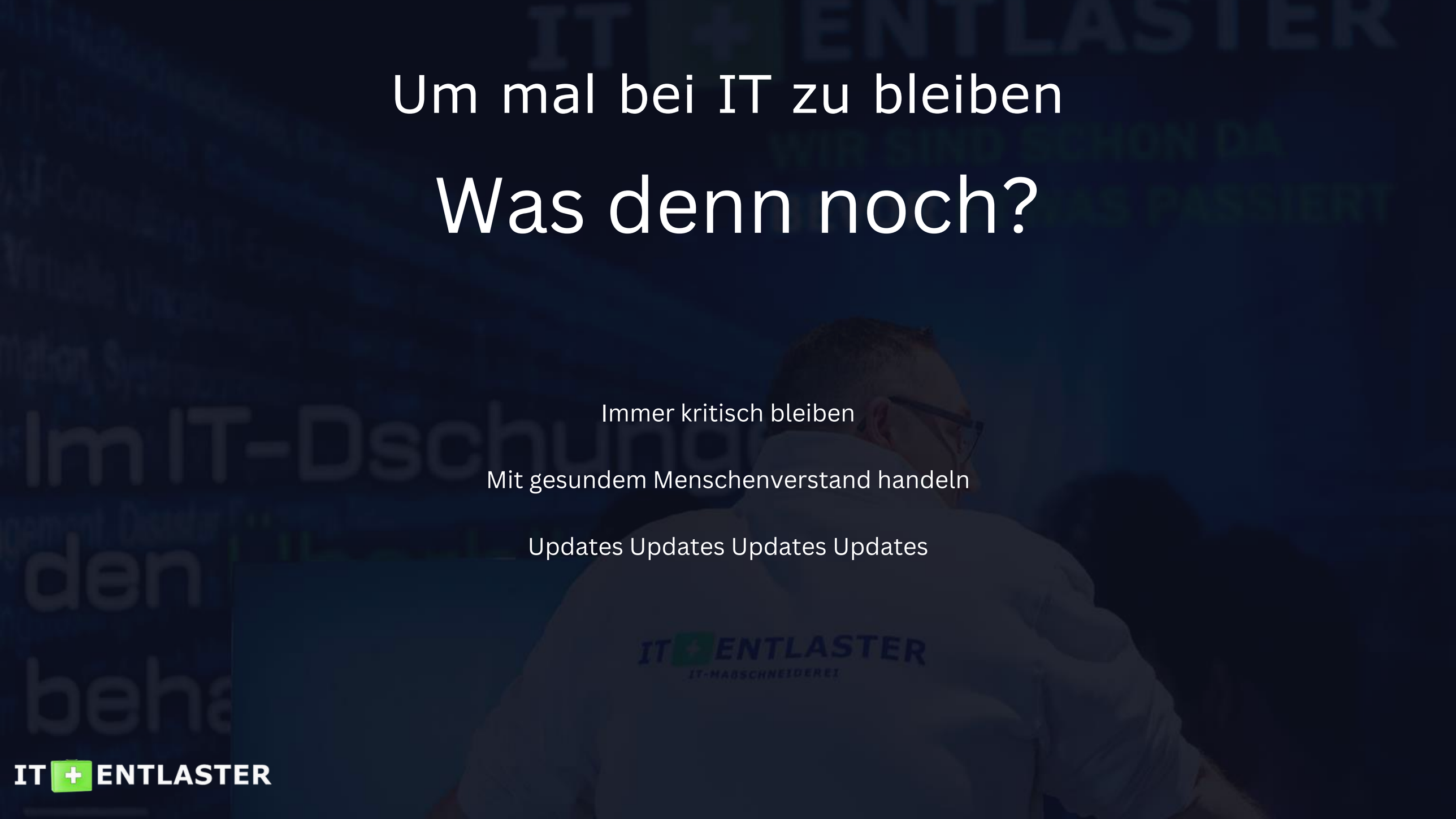
Um mal bei IT zu bleiben

Was denn noch?

Immer kritisch bleiben

Mit gesundem Menschenverstand handeln

Updates Updates Updates Updates



IT ENTLASTER

Um mal bei IT zu bleiben

Das ist doch alles ziemlich teuer oder?

Viele der von uns heute angesprochenen Dinge kosten kein Geld in Form von Lizenzen oder ähnlichem

Vieles ist organisatorischer Natur