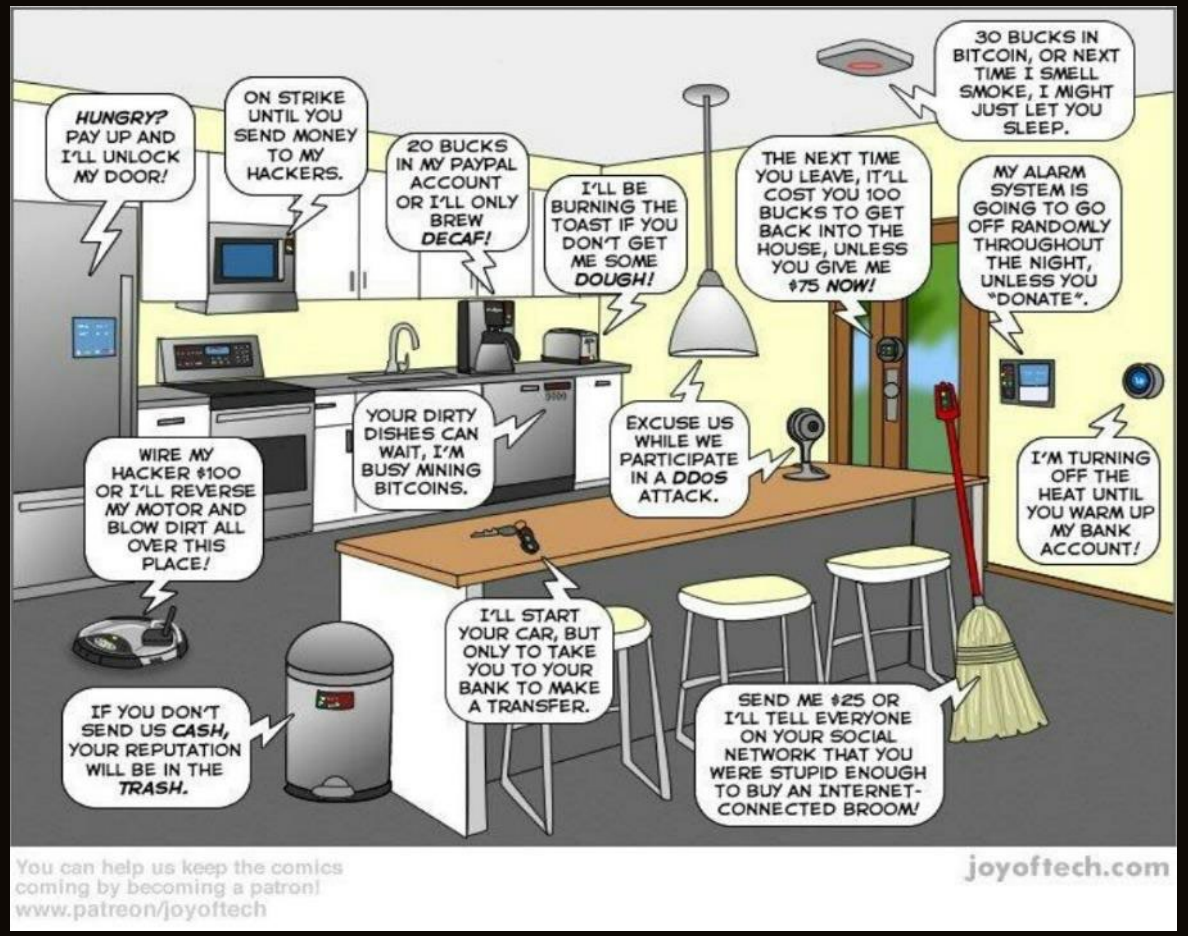
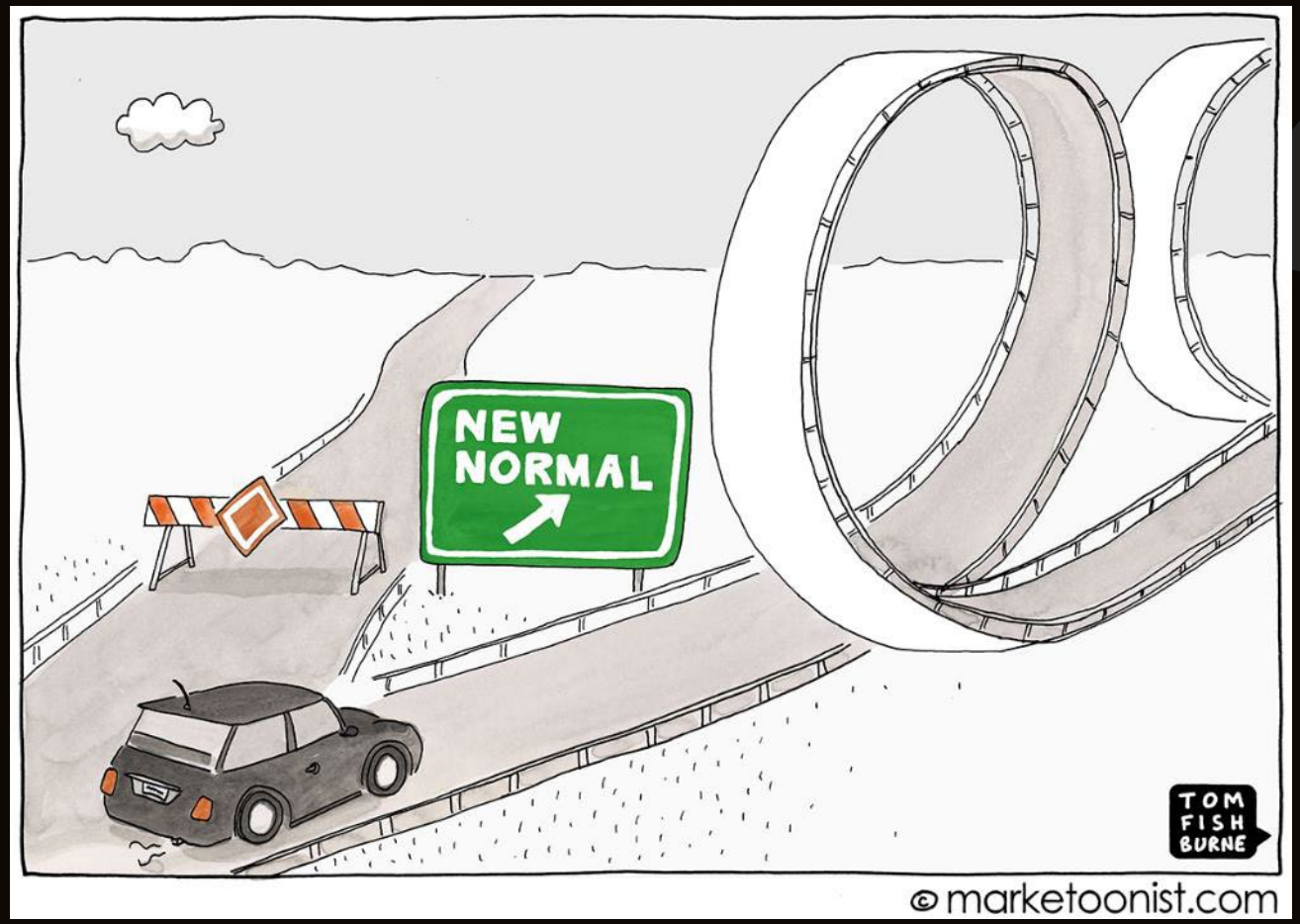
Stefan Dydak
Senior Security Advisor
August 2022

Mangelhaft: Endpunktsicherheit in Ausschreibungen

The Internet of Ransomware Things



Auf ins Abenteuer



Sicherheitsrisiken

In neuen und klassischen Arbeitsweisen

Immer mehr
RANSOMWARE
Angriffe

Neue Cyberkriminalität
CaaS

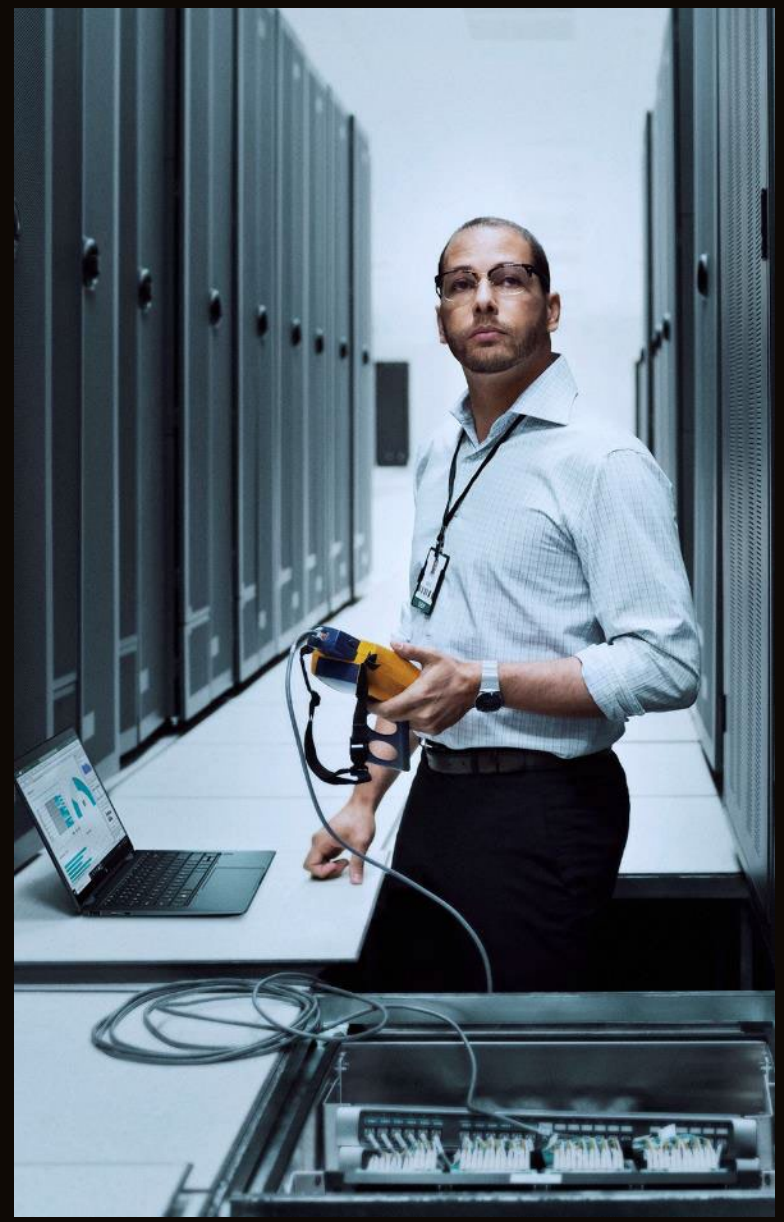
PRODUKTIVITÄT
über alles

HP WOLF SECURITY

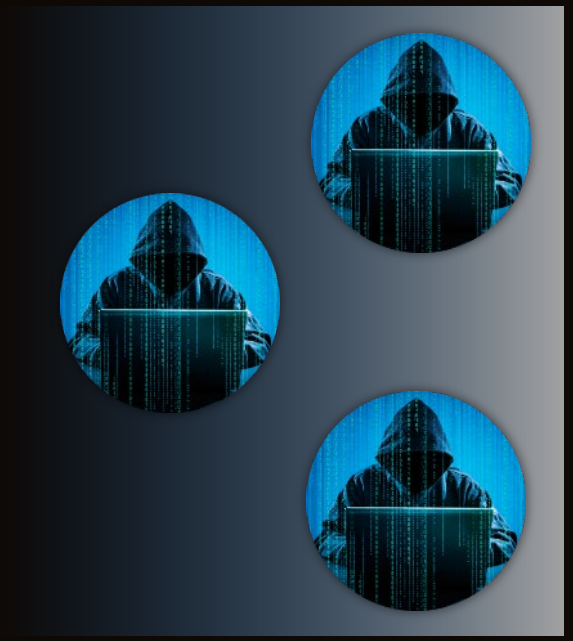
“

Drucker? Was kann da schon passieren?

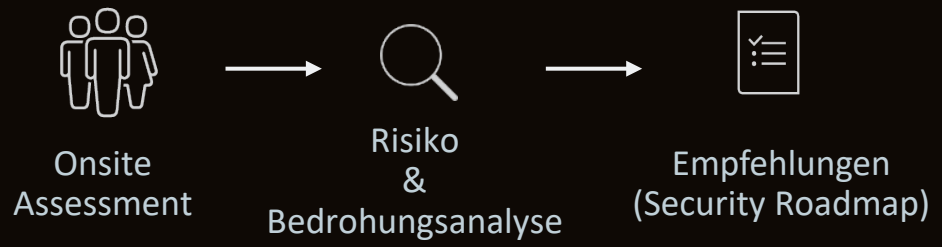
— CISO @ Black Hat

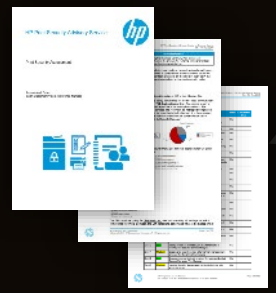


Endpunkte sind ein EINGANGSTOR



Was wir machen - Security Assessments





HP FRAMEWORK (ISO, NIST, HIPAA)	Compliance score
SA1 - Asset management	50%
SA2 - Configuration management	43%
SA3 - Data and document security	44%
SA4 - Logical access control	30%
SA5 - Security governance	50%
SA6 - Patching and Anti-Malware	33%
SA7 - Log Mgmt. and security incidents	17%
SA8 – Lifecycle Management	50%
Overall score	40%

SA5 - Security governance

8

Guter Wille – Mangelnde Ausführung

Die USB-Host-Ports sollen deaktiviert werden können und über Mechanismen verfügen, mit denen böswillige Angriffe verhindert werden können.

Authentifizierung und Berechtigung: Der Zugriff auf Gerätefunktionen muss über Rollen eingeschränkt werden können (z. B. Admin: Vollzugriff; User: Normale Benutzerrechte; Erweiterter User: Normale Benutzerrechte plus [redacted]

Filtern von TCP-Verbindungen: [redacted] können so konfiguriert werden, dass nur TCP-/IP-Verbindungen von festgelegten TCP-/IP-Adressen zulässig sind. [redacted]

Was alles schiefgeht?

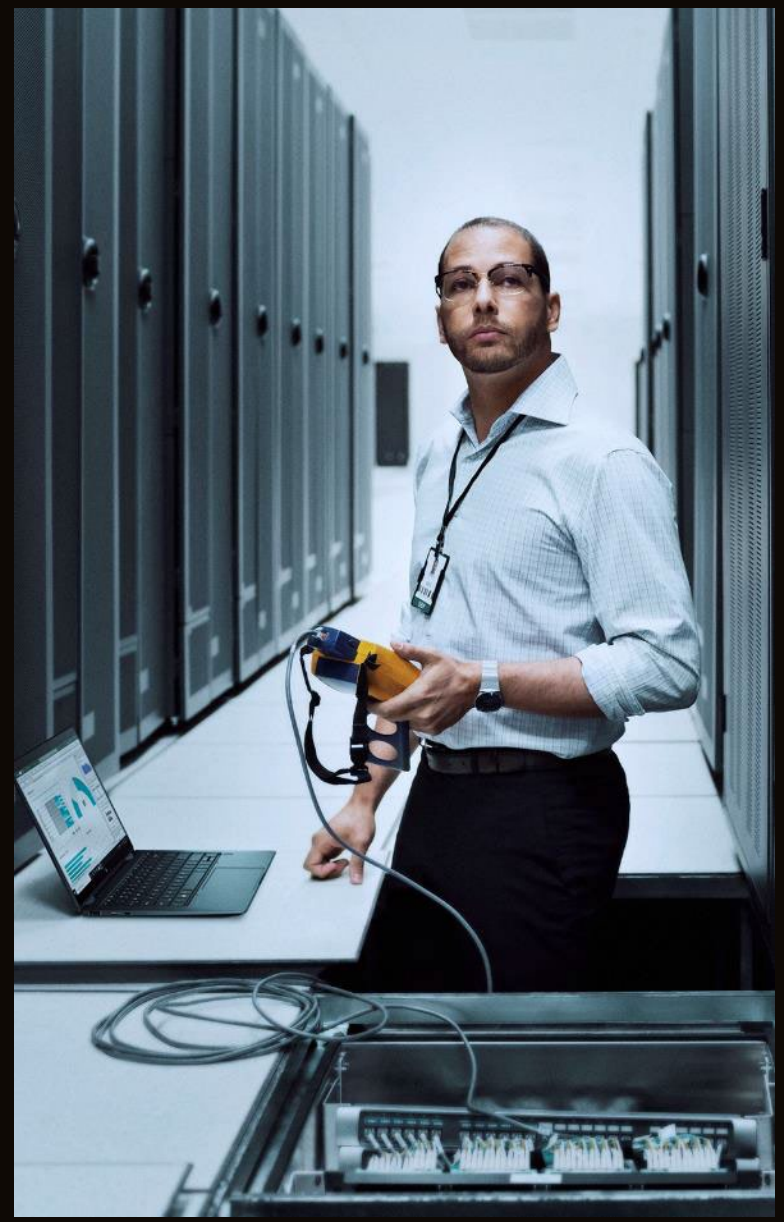
Die Wurzeln sind in der Beschaffung

- Abweichung zwischen Governance und Operations
- Decommissioning
- Shadow IT (Asset Management)
- Kein Monitoring
- Keine Härtung
- Mangelnde Privilegienkontrolle
- Kleinster gemeinsamer Nenner (Siehe IoT)
- Keine Haftung der Drittpartei

HP WOLF SECURITY

“

This means that the RFP and indeed the contract rarely explicitly require concrete security controls or services from the provider. As such the provider is **neither accountable nor responsible** for device hardening, data encryption, patching, compliance or security event monitoring and other typical security activities.



Ausschreibungen

Warum keine Sicherheit?

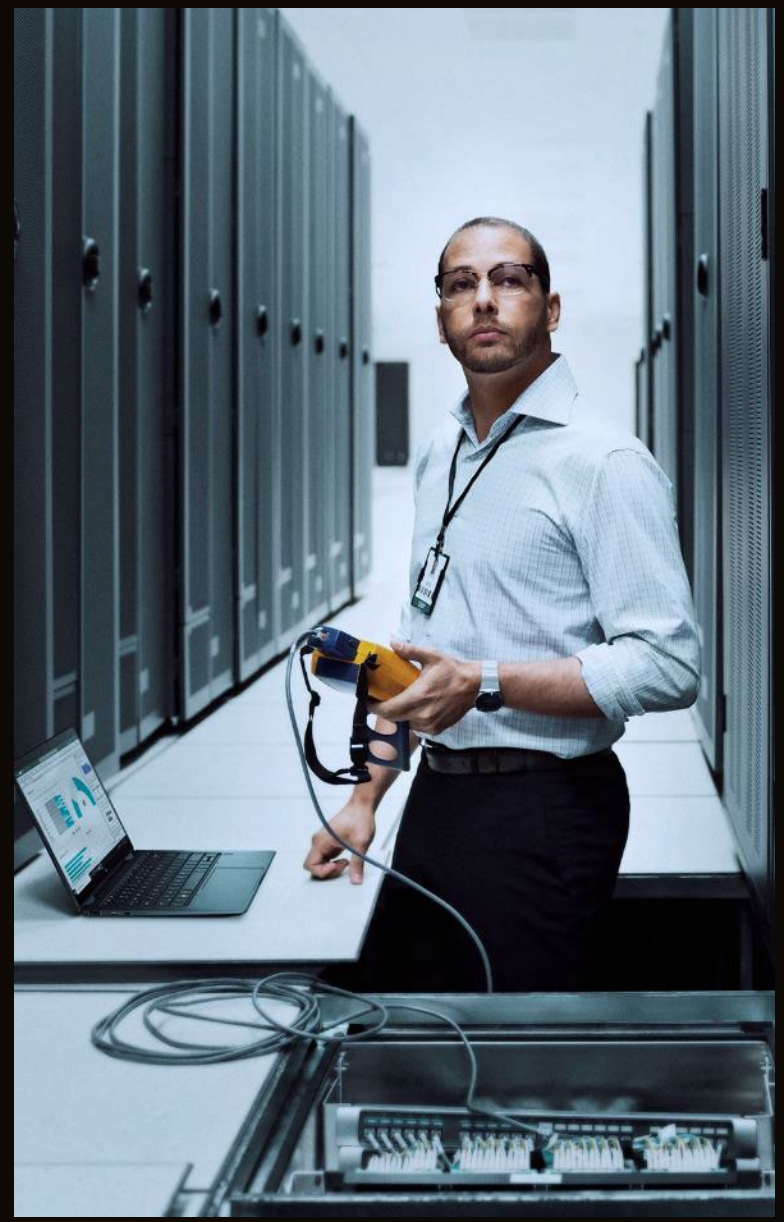
- Interaktion CISO - Einkauf?
- Andere Prioritäten?
- Fehlende Anpassung bei exotischeren Systemen?

Sicherheit wird zwar immer als Priorität genannt, aber die Details und SLAs fehlen oft.

HP WOLF SECURITY

“

For any future managed service, it is highly recommended to integrate **detailed security controls and requirements** into the contract and negotiate appropriate service level agreements (SLAs), thereby **outsourcing** at least some of **the** incurred **security risk** to the MPS provider.



Empfehlungen

- Die Sicherheitspolitik, Standards und Richtlinien des Unternehmens existieren schon. Sie müssen nur in Ausschreibungen integriert werden.
- Die Interaktion zwischen CISO und Einkauf sollte verstärkt werden.
- Jeder Einkauf muss wie ein Change behandelt und einer Gap / Risikoanalyse unterzogen werden.

Vielen Dank

Stefan Dydak
Senior Security Advisor
HP Inc