HP WOLF SECURITY

Präventive Endpoint-Sicherheit – Zeit für einen neuen Security Ansatz

heinz.maeurer@hp.com

HP WOLF SECURITY

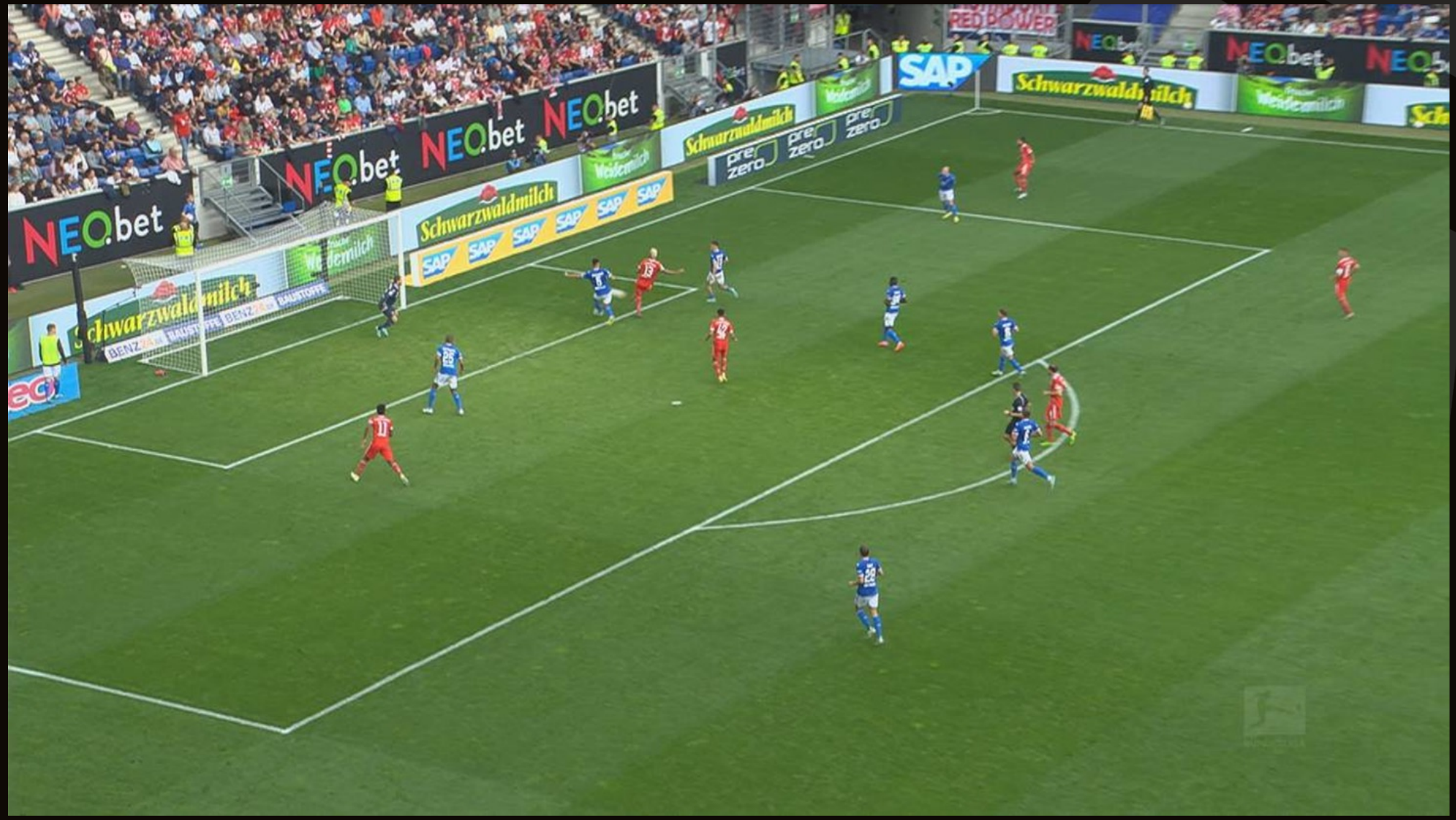
- IT Security – Allgemein betrachtet
  - Security Investment vs. Erfolg
  - Neue Ziele, alte Ziele neu entdeckt

- Closing the Gap mit HP Wolf Security

HP WOLF SECURITY

IT Security – Allgemein betrachtet

Eine Lücke reicht!



HP WOLF SECURITY

HP WOLF SECURITY

Etwas Statistik

In 2021 wurden in Deutschland rund 6,2 Milliarden Euro für IT-Sicherheit ausgegeben. Bis 2025 sollen rund 8,9 Milliarden Euro. (Quelle Statista 25.01.22)

Wohin geht das Geld?

EDR, XDR, NDR…

Email Security

Secure Web Gateway

SIEM, SOAR, SOC

PAM

DLP/DLD

Prozessoptimierung?

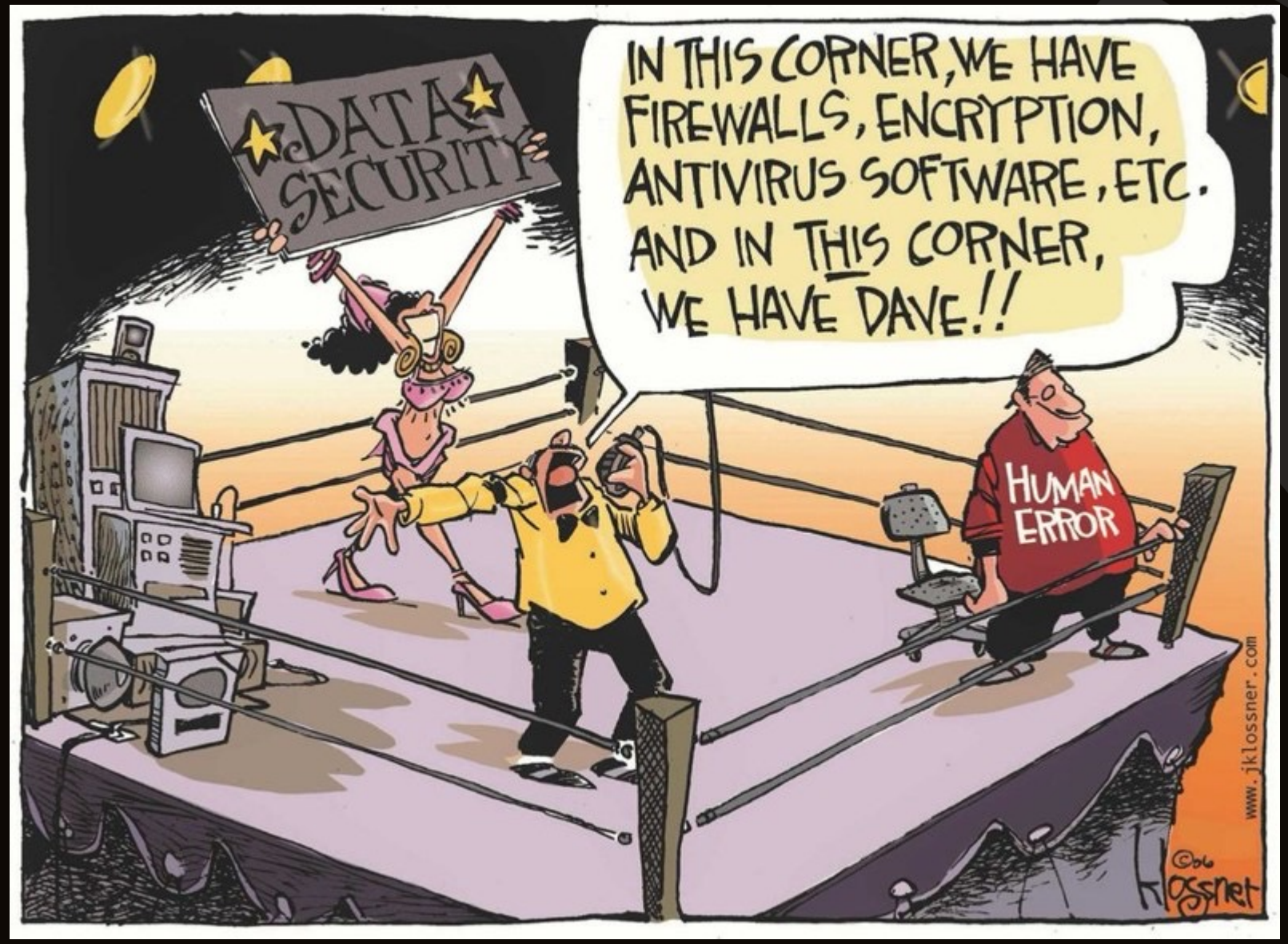
Mitarbeiterqualifikation?

Hardware Sicherheit?

Supply Chain Sicherheit?

Risk Assessments / Gap Analysen?

Risiko Mensch



Inherentes Risiko

Die Schnittstelle zwischen Mensch und Maschine bleibt Einstiegstor Nummer 1 – mehr als 85% aller Angriffe starten beim Faktor Mensch. Denn: Mitarbeitende lassen sich auch beim Einsatz der vielfältigsten Tools immer ähnlich angreifen – über emotionale Manipulation und Social Engineering.

Amateure hacken Systeme,
Profis hacken Menschen

- Bruce Schneier -

HP WOLF SECURITY

UND WAS SAGT DAS BSI DAZU?

Ausführung potentiell gefährlicher Inhalte in gekapselten Umgebungen

Eine weitere Schutzschicht kann die Ausführung potentiell gefährlicher Inhalte in gekapselten Umgebungen, insbesondere (Mirco-) VMs, sein. Dabei wird eine temporäre Arbeitsumgebung gestartet, welche regelmäßig wieder gelöscht oder zurückgesetzt wird. Wenn Dokumente und Dateien aus unsicheren Quellen in einer virtuellen Umgebung (VM) geöffnet werden, müsste entsprechende Schadsoftware aus dieser VM ausbrechen, um das eigentliche System zu infizieren. Entsprechende (Micro-) VMs können beispielsweise auch das Öffnen von Links aus E-Mails abdecken. Selbstverständlich müssen auch entsprechende Lösungen, welche (Micro-) Virtualisierung anbieten aktuell gehalten werden. Zum einen können Betriebssystem-Updates zu Problemen führen, zum anderen kann nur so verhindert werden, dass Schadprogramme aus der VM ausbrechen können

Quelle: BSI Maßnahmenkatalog Ransomware - Arbeitspapier