INDUSTRIE 4.0

SAFETY UND SECURITY

mbt
maschinenbautage
mechtersheimer

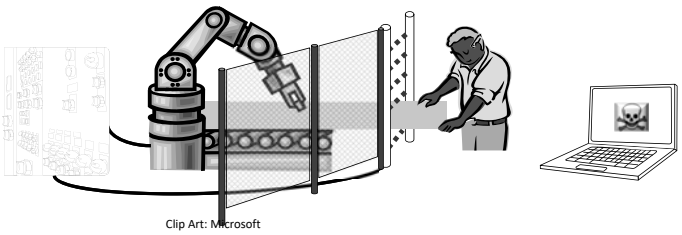
Safety / Security

Safety

- Der Schutz vor der Maschine
- Risikobeurteilung:
  Schaden durch Maschine

Security

- Der Schutz der Maschine
- Risikobeurteilung:
  Schaden an der Maschine



Clip Art: Microsoft

Safety / Security

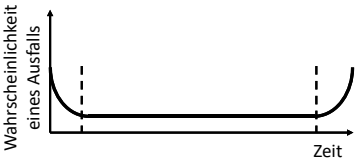
Safety

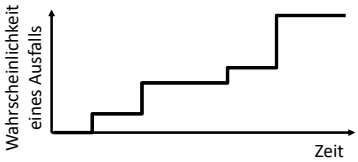
- Lineare Ausfallrate
- Numerische PL (13849), SIL (62061)

Security

- Zufällig ansteigende Ausfallrate
- Qualitative SL* (62443)

* Security Level





Wer ist (mit)schuld?

- Hersteller
- Händler
- Arbeitgeber
- Benutzer

Wer ist schuld?

"Every kind of (external) intentional violation (sabotage/spying) of a machine is de facto a criminal act which is outside the scope of current safety legislation and consequently of standardization for machinery safety which is supporting this legislation."

- Hersteller
- Händler
- Arbeitgeber
- Benutzer

VDMA in ISO/NP TR 22100-4:2017-08 Absatz 5.1

Wer ist schuld?

Übersetzt:
Hacken ist kriminell.
MRL und EN ISO 12100 decken kriminelle Handlungen nicht ab.

VDMA in ISO/NP TR 22100-4:2017-08

- Hersteller
- Händler
- Arbeitgeber
- Benutzer

Wer ist schuld?

„Oder bin ich verpflichtet, an meinem neuen Auto erstmal die Türschlösser zu tauschen, weil VW überall dasselbe Schloss verbaut?“

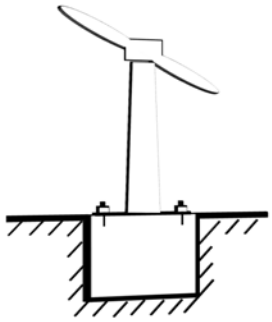
https://forum.golem.de/kommentare/security/internet-of-things-bricker-bot-soll-2-millionen-iot-geraete-zerstoert-haben/herstellerhaftung/108886,4793445,4793445,read.html#msg-4793445

- Hersteller
- Händler
- Arbeitgeber
- Benutzer

Neue und härtere Gesetze!!!

- MRL
- BGB / HGB
- BetrSichV

Neue und härtere Gesetze!!!



BSI* (zu golem.de):

"*Uns sind keine Gesetze bekannt, die die Einhaltung von IT-Sicherheitsstandards für Windkraftanlagen mit einer Nettonennleistung von unter 420 MW fordern.*"

*Bundesamt für Sicherheit in der Informationstechnik

MRL zu Security

„Der Hersteller oder sein Bevollmächtigter muss vor dem Inverkehrbringen und/oder der Inbetriebnahme einer Maschine

a) sicherstellen, dass die Maschine die in Anhang I aufgeführten, **für sie geltenden grundlegenden Sicherheits- und Gesundheitsschutzanforderungen** erfüllt;“

- Artikel 5 (1) a)

MRL zu Security

„Der Hersteller oder sein Bevollmächtigter muss vor dem Inverkehrbringen und/ Inbetriebnah

a) sie die **sie Sich Gesundheitsschutzanforderungen** erfüllt;“

Maschine muss GSA einhalten

- Artikel 5 (1) a)

MRL zu Security

„Die mit den grundlegenden Sicherheits- und Gesundheitsschutzanforderungen verbundenen Verpflichtungen gelten nur dann, wenn an der betreffenden Maschine bei Verwendung unter den vom Hersteller oder seinem Bevollmächtigten vorgesehenen Bedingungen oder unter vorhersehbaren ungewöhnlichen Bedingungen die entsprechende Gefährdung auftritt. […]“

- Artikel 5 (1) a)
- Anhang I Allgemeine Grundsätze 2.

MRL zu Security

„Die mit den grundlegenden Sicherheits- und Gesundheit… … sprechende Gefähr… …ftritt. […]“

GSA gilt nur, wenn die Gefährdung unter **vorhersehbaren (ungewöhnlichen) Bedingungen** auftritt

- Artikel 5 (1) a)
- Anhang I Allgemeine Grundsätze 2.

MRL zu Security

„Steuerungen sind so zu konzipieren und zu bauen, dass es nicht zu Gefährdungssituationen kommt. Insbesondere müssen sie so ausgelegt und beschaffen sein, dass

- sie den zu erwartenden Betriebsbeanspruchungen und Fremdeinflüssen standhalten;
- ein Defekt der Hardware oder der Software der Steuerung nicht zu Gefährdungssituationen führt;
- […]“

- Artikel 5 (1) a)
- Anhang I Allgemeine Grundsätze 2.
- MRL Anhang I
  - 1.2.1.

MRL zu Security

„Steuerungen sind so zu konzipieren und zu bauen, dass es nicht zu Gefährdungssituationen kom… Insbesondere müss… …nd beschaffen… …der …rung nicht zu …ngssituationen führt;

- […]“

Steuerungen dürfen bei **Fremdeinfluss und Softwarefehler** nicht gefährden

- Artikel 5 (1) a)
- Anhang I Allgemeine Grundsätze 2.
- MRL Anhang I
  - 1.2.1.

MRL zu Security

„Jede Betriebsanleitung muss erforderlichenfalls folgende Mindestangaben enthalten:

l) Angaben zu Restrisiken, […]

r) Beschreibung der vom Benutzer durchzuführenden Einrichtungs- und Wartungsarbeiten […]

s) Anweisungen zum sicheren Einrichten und Warten […]“

- Artikel 5 (1) a)
- Anhang I Allgemeine Grundsätze 2.
- MRL Anhang I
  - 1.2.1.
  - 1.7.4.2. l) r) s)

MRL zu Security

„Jede Betriebsanleitung muss erforderlichenfalls folgende Mindestangaben enthal… l) Angaben … …ungs- …beiten […] s) …weisungen zum sicheren Einrichten und Warten […]“

Restrisiken und Wartung (Updates) müssen in BA beschrieben sein

- Artikel 5 (1) a)
- Anhang I Allgemeine Grundsätze 2.
- MRL Anhang I
  - 1.2.1.
  - 1.7.4.2. l) r) s)

BGB/HGB zu Mangel

Die Sache ist frei von Sachmängeln, wenn sie bei Gefahrübergang die vereinbarte Beschaffenheit hat. Soweit die Beschaffenheit nicht vereinbart ist, ist die Sache frei von Sachmängeln,

1. wenn sie sich für die nach dem Vertrag vorausgesetzte Verwendung eignet, sonst
2. wenn sie sich für die gewöhnliche Verwendung eignet und eine Beschaffenheit aufweist, die bei Sachen der gleichen Art üblich ist und die der Käufer nach der Art der Sache erwarten kann.

[…]

- §§ 434ff BGB

BGB/HGB zu Mangel

Die Sache ist frei von Sachmängeln, wenn sie bei Gefahrübergang die vereinbarte Beschaffenheit hat. Soweit die Beschaffenheit nicht [illegible] art ist, ist die Sache frei von [illegible]

1. wenn sie [illegible]

Maschine muss sich für Verwendung (evtl. Internet) eignen

[illegible] die bei Sachen der [illegible] ist und die der Käufer [illegible] Art der Sache erwarten kann.

[…]

- §§ 434ff BGB

BGB/HGB zu Mangel

(1) Die in § 437 Nr. 1 und 3 bezeichneten Ansprüche verjähren
   […]
   3. im Übrigen in zwei Jahren.

(2) Die Verjährung beginnt […] mit der Ablieferung der Sache.

[…]

- §§ 434ff BGB
- § 438 BGB
  + § 634a BGB (1,2)

BGB/HGB zu Mangel

(1) Die in § 437 Nr. 1 und [illegible] bezeichnet[illegible]

Ansprüche verfallen 2 Jahre nach Übergabe. Bei Individualsoftware 2 Jahre nach Abnahme.

[illegible] ren.

(2) [illegible] beginnt […] mit [illegible] Ablieferung der Sache.

[…]

- §§ 434ff BGB
- § 438 BGB
  + § 634a BGB (1,2)

BGB/HGB zu Mangel

(1) Ist der Kauf für beide Teile ein Handelsgeschäft, so hat der Käufer die Ware unverzüglich nach der Ablieferung durch den Verkäufer, soweit dies nach ordnungsmäßigem Geschäftsgang tunlich ist, zu untersuchen und, wenn sich ein Mangel zeigt, dem Verkäufer unverzüglich Anzeige zu machen.

- §§ 434ff BGB
- § 438 BGB
  + § 634a BGB (1,2)
- § 377 HGB

BGB/HGB zu Mangel

(1) Ist der Kauf für beide Teile ein Handelsgeschäft, so hat der Käufer die Ware unv[illegible] nach der Ab[illegible] [illegible]n Verk[illegible]

In B2B ~~Abnahme~~ Mängelrüge so bald wie möglich

[illegible] ist, zu [illegible] und, wenn sich ein M[illegible]ngel zeigt, dem Verkäufer unverzüglich Anzeige zu machen.

- §§ 434ff BGB
- § 438 BGB
  + § 634a BGB (1,2)
- § 377 HGB

BGB/HGB zu Mangel

(2) Unterläßt der Käufer die Anzeige, so gilt die Ware als genehmigt, es sei denn, daß es sich um einen Mangel handelt, der bei der Untersuchung nicht erkennbar war.

- §§ 434ff BGB
- § 438 BGB
  + § 634a BGB (1,2)
- § 377 HGB

BGB/HGB zu Mangel

(2) Unterläßt der Käufer die Anzeige, so gilt die W genehmigt bei der Untersuchung nicht erkennbar war.

Nicht gemeldete Mängel sind akzeptiert.

- §§ 434ff BGB
- § 438 BGB
  + § 634a BGB (1,2)
- § 377 HGB

BGB/HGB zu Mangel

(3) Zeigt sich später ein solcher Mangel, so muß die Anzeige unverzüglich nach der Entdeckung gemacht werden; anderenfalls gilt die Ware auch in Ansehung dieses Mangels als genehmigt.

- §§ 434ff BGB
- § 438 BGB
  + § 634a BGB (1,2)
- § 377 HGB

BGB/HGB zu Mangel

(3) Zeigt sich später ein solcher Mangel, so mu unv ; die Ware a in Ansehung dieses Mangels als genehmigt.

Mängel, die später auftauchen sind bei Entdeckung zu melden.

- §§ 434ff BGB
- § 438 BGB
  + § 634a BGB (1,2)
- § 377 HGB

BGB/HGB zu Mangel

(5) Hat der Verkäufer den Mangel arglistig verschwiegen, so kann er sich auf diese Vorschriften nicht berufen.

§ 195
Die regelmäßige Verjährungsfrist beträgt drei Jahre.

- §§ 434ff BGB
- § 438 BGB
  + § 634a BGB (1,2)
- § 377 HGB
  + § 195 HGB
  + § 634a (3)

BGB/H Mangel

(5) Hat d ch

§ 19
Die r gsfrist
beträ

Wenn der Mangel dem Verkäufer **bekannt** sein musste und **verschwiegen** wurde haftet er für 3 Jahre. Ein vereinbarter Haftungsausschluss ist unwirksam.

- §§ 434ff BGB
- § 438 BGB
  + § 634a BGB (1,2)
- § 377 HGB
  + § 195 HGB
  + § 634a (3)

BGB/HGB zu Mangel

(1) Verletzt der Schuldner eine Pflicht aus dem Schuldverhältnis, so kann der Gläubiger Ersatz des hierdurch entstehenden Schadens verlangen. Dies gilt nicht, wenn der Schuldner die Pflichtverletzung nicht zu vertreten hat.

- §§ 434ff BGB
- § 438 BGB
  + § 634a BGB (1,2)
- § 377 HGB
  + § 195 HGB
  + § 634a (3)
- § 280 BGB

BGB/HGB zu Mangel

(1) Verletzt der Schuldner eine Pflicht aus dem Schuldv[illegible] er [illegible] gilt [illegible] Schuldner die P[illegible]ntverletzung nicht zu vertreten hat.

Wenn der (Secutity-) Mangel zu einem Schaden führt, muss der Verkäufer Ersatz leisten

- §§ 434ff BGB
- § 438 BGB
  + § 634a BGB (1,2)
- § 377 HGB
  + § 195 HGB
  + § 634a (3)
- § 280 BGB

BGB/HGB zu Mangel

(1) Die Rechte des Käufers wegen eines Mangels sind ausgeschlossen, wenn er bei Vertragsschluss den Mangel kennt […]

- §§ 434ff BGB
- § 438 BGB
  + § 634a BGB (1,2)
- § 377 HGB
  + § 195 HGB
  + § 634a (3)
- § 280 BGB
- § 442 BGB

BGB/HGB zu Mangel

(1) Die R[illegible] [illegible]ren

Wenn der Käufer wissentlich eine Maschine mit (Security-) Mängeln kauft hat er keine Ansprüche

- §§ 434ff BGB
- § 438 BGB
  + § 634a BGB (1,2)
- § 377 HGB
  + § 195 HGB
  + § 634a (3)
- § 280 BGB
- § 442 BGB

BetrSichV

§4

(1) Arbeitsmittel dürfen erst verwendet werden, nachdem der Arbeitgeber […]

3. festgestellt hat, dass die Verwendung der Arbeitsmittel nach dem Stand der Technik sicher ist.

§2

(10) Stand der Technik ist der Entwicklungsstand fortschrittlicher […] Betriebsweisen, der die praktische Eignung einer Maßnahme […] zum Schutz der Gesundheit und zur Sicherheit der Beschäftigten oder anderer Personen gesichert erscheinen lässt. Bei der Bestimmung des Stands der Technik sind insbesondere vergleichbare […] Betriebsweisen heranzuziehen, die mit Erfolg in der Praxis erprobt worden sind.

- §4 (1) 3.
- §2 (10)

BetrSichV

§4

(1) Arbeitsmittel dürfen erst verwendet werden, nachdem der Arbeitgeber […]

3. festgestellt hat, dass die [illegible] nach dem Stand der T[illegible]

§2

(1[illegible] [illegible] zum Schutz [illegible]heit der Beschäftigten [illegible] gesichert erscheinen lässt. [illegible]mmung des Stands der Technik sind i[illegible]esondere vergleichbare […] Betriebsweisen heranzuziehen, die mit Erfolg in der Praxis erprobt worden sind.

Maschinen müssen nach dem Stand der Technik sicher sein

- §4 (1) 3.
- §2 (10)

BetrSichV

§3

(7) Die Gefährdungsbeurteilung ist regelmäßig zu überprüfen. Dabei ist der Stand der Technik zu berücksichtigen. Soweit erforderlich, sind die Schutzmaßnahmen bei der Verwendung von Arbeitsmitteln entsprechend anzupassen. […]

- §4 (1) 3.
- §2 (10)
- §3 (7)

BetrSichV

§3

(7) Die Gefährd… ist … k … der … von Arbeitsmitteln e…prechend anzupassen. […]

Maschinen müssen regelmäßig auf eine Sicherheit nach Stand der Technik geprüft werden

- §4 (1) 3.
- §2 (10)
- §3 (7)

BetrSichV

§10

(1) Der Arbeitgeber hat Instandhaltungsmaßnahmen zu treffen, damit die Arbeitsmittel während der gesamten Verwendungsdauer den für sie geltenden Sicherheits- und Gesundheitsschutzanforderungen entsprechen und in einem sicheren Zustand erhalten werden. […]

- §4 (1) 3.
- §2 (10)
- §3 (7)
- §10 (1)

BetrSichV

§10

(1) Der Arbeitgeber h… Instandh… zu … el … und in einem s… Zustand erhalten werden. […]

Maschinen müssen regelmäßig auf eine Sicherheit nach Stand der Technik gebracht werden

- §4 (1) 3.
- §2 (10)
- §3 (7)
- §10 (1)

Rechtsfolgen

- Ein Softwarefehler (Bug), bezeichnet im Allgemeinen ein Fehlverhalten von Computerprogrammen.
- Dies tritt auf, wenn der Programmierer eine bestimmte Festlegung der Spezifikation nicht oder falsch umgesetzt hat, oder wenn die Laufzeitumgebung fehlerhaft bzw. anders als erwartet arbeitet. Dies stellt einen Mangel dar.
- Nicht aktuelle Software kann ebenfalls einen Mangel darstellen.

Rechtsfolgen

- Besitzt eine Maschine einen Kommunikationsanschluss, der dafür geeignet ist, sie in ein Netzwerk einzubinden, sind generell Viren und andere Schadprogramme typische zu erwartende Fremdeinflüsse.
- Schadprogramme zielen regelmäßig auf bekannte Sicherheitslücken ab.
- Für solche Sicherheitslücken bestehen im Internet frei einsehbare Datenbanken, so dass Verkäufer und Käufer sich über die Risiken der eingesetzten Programme informieren können.

Rechtsfolgen

- Nach § 377 HGB hat der Käufer die Pflicht, im Rahmen einer Funktionsprüfung auch die Software auf Fehler zu prüfen. Vorhandene nicht angezeigte Softwaremängel gelten als akzeptiert.
- Typischerweise werden in selbst entwickelter Software Dritt-Programme integriert. Diese sind für den Käufer schwer bis gar nicht zu identifizieren.
- Wird ein Mangel in einer (Dritt-)Software erst später ersichtlich, hat der Käufer dem Verkäufer dies unverzüglich nach Entdeckung anzuzeigen. Auch wenn er vorher nichts angezeigt hat, muss der Verkäufer den zusätzlichen Mangel beheben (Gewährleistung).

Rechtsfolgen

- Spätestens nach Ablauf von 2 Jahren (3 Jahre für arglistig verschwiegene Fehler) muss sich der Betreiber selbst um Security-Updates kümmern.
- Da dies i.d.R. nicht möglich ist muss er Ersatzmaßnahmen treffen, um gleichwertige Sicherheit nach dem Stand der Technik zu gewährleisten.

Rechtsfolgen

- Da MRL Anhang I 1.2.1. eine gesetzliche Pflicht ist, kann sie nicht privatvertraglich ausgehebelt werden.
- Liefert ein Verkäufer eine Maschine vertragsgemäß mit Software mit allgemein bekannten Sicherheitslücken (z.B. Win XP), ist dies ein Mangel.
- Ein solcher Mangel gilt dann als dem Käufer bei Vertragsabschluss bekannt.

Rechtsfolgen

- Da MRL Anhang I 1.2.1 ne gesetzliche Pflicht ist, kann sie traglich ausgehebelt
- Ein solcher Mange dem Käufer bei Vertragsabschluss b nnt.

Verkäufer darf nach ProdSG nicht liefern

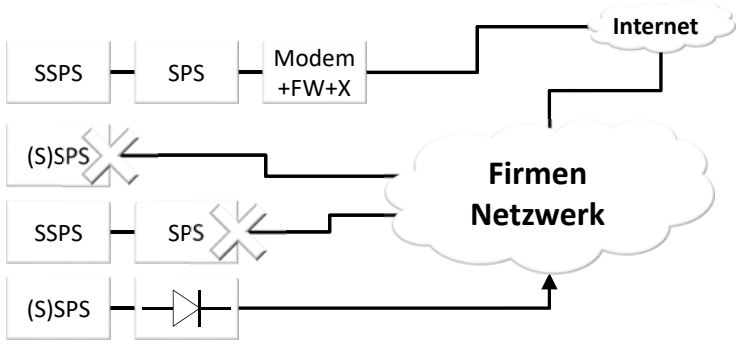
Betreiber darf nach BetrSichV nicht nutzen

Betreiber ~~darf~~ kann nach BGB nicht rügen

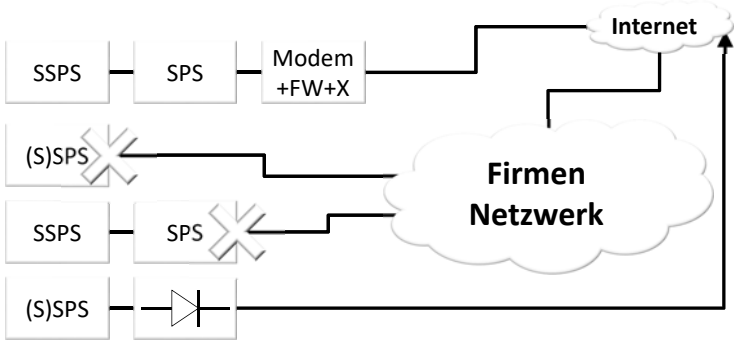
(S)SPS als Opfer

- SPS und SSPS werden angegriffen

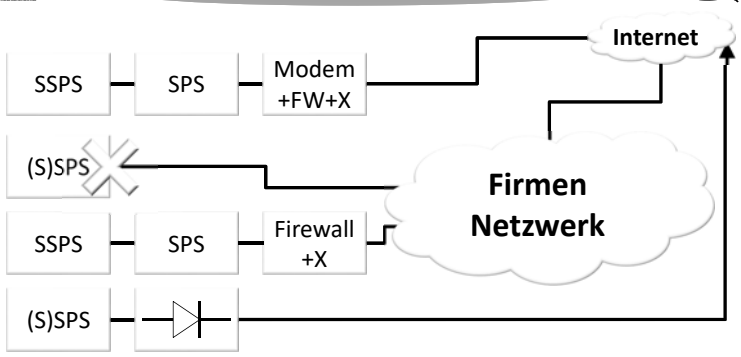
Lösungen für KMU



Lösungen für KMU



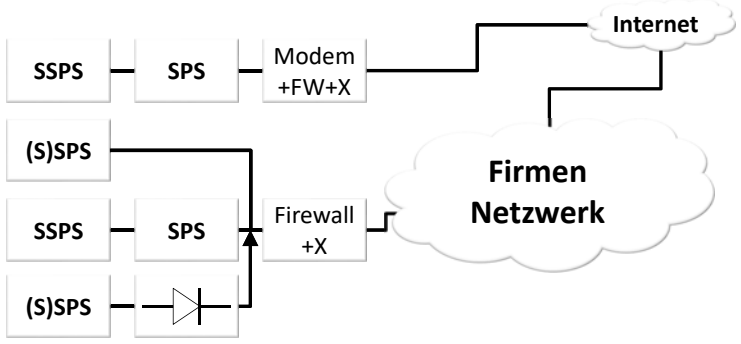
Lösungen für KMU



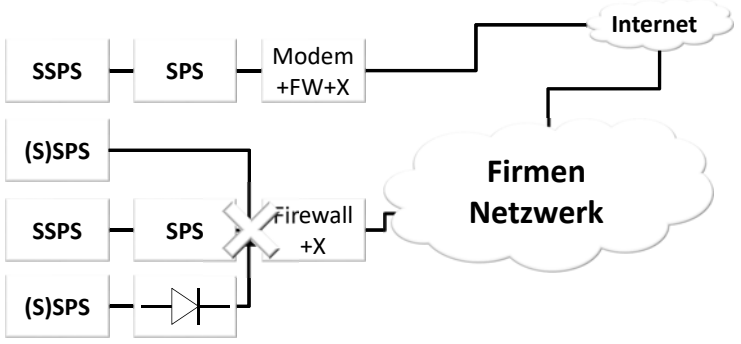
(S)SPS als Täter

- SPS und SSPS greifen an

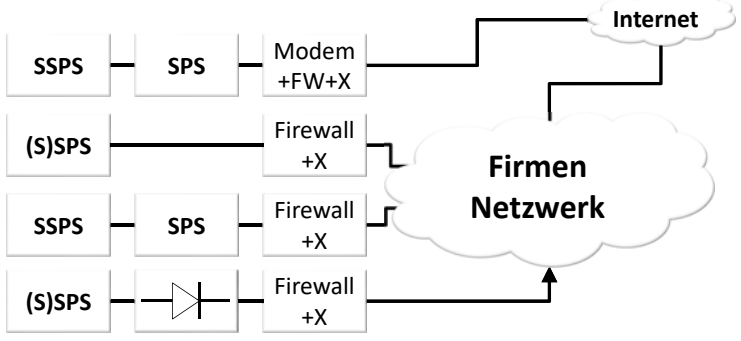
Lösungen für KMU



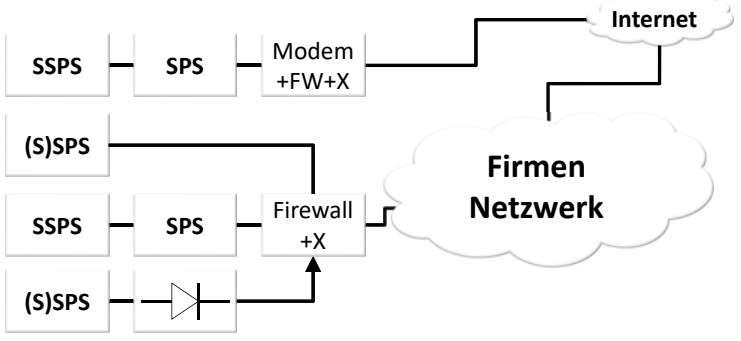
Lösungen für KMU



Lösungen für KMU



Lösungen für KMU



Wieviel X darf es sein?

- Rendezvous Server
  - mit Aufzeichnung
- Netzwerk Analyse
  - Wer mit wem?
  - Wann?
  - Welcher Inhalt?
- Virenscanner

Links

- CC-BY
  - 2.0: https://creativecommons.org/licenses/by/2.0/
  - SA 3.0: https://creativecommons.org/licenses/by-sa/3.0/de/
- Problemkinder:
  - https://www.heise.de/security/meldung/Zwei-Jahre-alte-Sicherheitsluecken-in-Tomografen-von-Siemens-3793673.html
- Wen interessiert's?:
  - https://www.golem.de/news/netzsicherheit-weltweiter-hackerangriff-koennte-53-milliarden-dollar-kosten-1707-128963.html
    http://www.spiegel.de/wirtschaft/unternehmen/cyberangriffe-auf-deutsche-firmen-verursachen-milliardenschaeden-a-1158975.html
    https://www.heise.de/security/meldung/Cyber-Attacke-NotPetya-Unternehmen-haben-immer-noch-viel-Arbeit-mit-dem-Fallout-des-Angriffs-3782794.html
    https://www.golem.de/news/wannacry-nsa-exploits-legen-weltweit-windows-rechner-lahm-1705-127801.html
    https://www.golem.de/news/deutsche-bahn-schadsoftware-lasst-anzeigetafeln-auf-bahnhoefen-ausfallen-1705-127802.html
    https://www.heise.de/newsticker/meldung/WannaCry-Zehntausende-Tankstellen-in-China-offline-Deutsche-Bahn-behebt-Schaeden-3714259.html
  - https://www.heise.de/newsticker/meldung/Malware-auf-Zerstoerungspfad-Brickerbot-legt-unsichere-IoT-Geraete-still-3678861.html
    https://www.washingtonpost.com/news/the-intersect/wp/2017/04/09/someone-hacked-every-tornado-siren-in-dallas-it-was-loud/?tid=sm_tw&utm_term=.46af97906639
    http://www.kta.de/koeln/nach-sirenen-hack-in-troisdorf-sirenen-in-koeln-sollen-gegen-angriff-gesichert-sein-24744ef4j
  - https://www.heise.de/newsticker/meldung/Auftrag-kam-aus-Liberia-Der-Hacker-der-Telekom-Router-sagt-aus-3780499.html
    http://www.spiegel.de/netzwelt/netzpolitik/telekom-hack-brite-in-koeln-zu-bewaehrungsstrafe-verurteilt-a-1160149.html
- Wer greift an?:
  - https://www.heise.de/ix/heft/Klein-aber-gemein-3754482.html
    http://www.taz.de/!5307828/
    https://www.heise.de/newsticker/meldung/Schweden-Regierungsdaten-in-der-Cloud-mit-eingebauter-Sicherheitsluecke-3782202.html
    https://www.heise.de/security/artikel/Die-Geschichte-von-Junipers-entwendeter-Hintertuer-3794610.html
- Wie viele greifen woher an?
  - https://www.heise.de/newsticker/meldung/Ueber-47-Millionen-IT-Angriffe-auf-die-Bundeswehr-im-Jahr-2016-3595632.html
    https://www.heise.de/forum/heise-online/News-Kommentare/Von-der-Leyen-Grosse-Fortschritte-bei-Cyber-Sicherheit/4501-Angriffe-taeglich-auf-die-Bundeswehr/posting-31013551/show/
    https://www.heise.de/newsticker/meldung/Von-der-Leyen-Grosse-Fortschritte-bei-Cyber-Sicherheit-3825984.html
- Woher kommt das Problem?
  - https://www.heise.de/newsticker/meldung/Sicherheitslaecke-in-Am-Siegerwahlgeraeten-mit-Bildschirmanzeige-3770629.html
    https://www.heise.de/newsticker/meldung/Gezielte-Fuzzing-Angriffe-auf-Bahnhofsanzeigetafeln-3768878.html
    https://www.golem.de/news/spiegel-war-hacktivisten-angriff-auf-deutsche-bahn-1708-127906.html
    https://www.heise.de/newsticker/meldung/Ransomware-Angriff-auf-Bahnhofsanzeigen-mit-Windows-XP-3771767.html
    https://www.heise.de/newsticker/meldung/Ueber-1000-Jahre-alte-Kirchenglocken-mit-Ransomware-infiziert-3771767.html
    https://www.heise.de/newsticker/meldung/Ransomware-Emotet-ein-ein-Virus-wird-zum-Trojaner-3772450.html
    https://www.golem.de/news/ransomware-emotet-ein-ein-virus-wird-zum-trojaner-1707-128147.html
    https://www.heise.de/ct/artikel/Wie-Angreifer-Web-Browser-und-Mail-Clients-hacken-3800225.html
    https://www.heise.de/ct/artikel/Ein-Jahr-Cyber-Angriffe-auf-Bundeswehr-3825984.html
    https://www.heise.de/newsticker/meldung/20-Jahre-Zehnfaktor-Gesetze-Wie-sicherer-wurde-es-aus-Unternehmen-3827586.html
    http://www.golem.de/news/hitrust-cyber-risk-assessment-1708-128224.html
    http://www.heise.de/ct/artikel/Ein-Jahr-Cyber-Angriffe-auf-Bundeswehr-3825984.html
- Wer ist schuld?
  - https://www.golem.de/news/internet-of-things-dildos-sollen-smart-sein-duerfen-1704-127150.html
- BGB/HGB zu Mangel
  - http://www.frag-einen-anwalt.de/Dauer-bzw-Ausschluss%C3%9F-Gewaehrleistung-bei-Internetentwicklung--f43794.html


```
Starting Nmap 7.01 ( https://nmap.org  ) at 2017-10-01 13:37 EST
Nmap scan report for 127.0.0.1
Host is up (0.0000001s latency).
PORT     STATE    SERVICE
515/tcp  closed   printer
631/tcp  closed   ipp

Nmap scan report for 192.168.0.1
Host is up (0.1337s latency).
PORT     STATE    SERVICE
515/tcp  open     printer
631/tcp  open     ipp

Nmap done: 256 IP addresses (2 hosts up) scanned in 13.37 seconds
```