Neue Herausforderungen in einer vernetzten Welt – aktuelle Bedrohungen und neue Anforderungen

THORSTEN RÖDEL
PECB CERTIFIED ISO/IEC, 27001 LEAD AUDITOR UND IMPLEMENTER

GEMEINSAM GESTALTEN WIR
IHREN DIGITALEN WANDEL

FRÜHER

- Früher waren Firewall und AV meist ausreichend
- Die Angriffe eher sporadisch
- Spam war überschaubar

HEUTE

- Firewall und AV meist nicht ausreichend
- Die Angriffe nehmen überhand
- Spam wird zum echten Problem für viele Filter
- Angriffe kommen im Minutentakt, von überall
- Selbst mein Fernseher hackt mich mittlerweile

STATUS

- Privatpersonen sind überwiegend überfordert damit, Ihre Systeme abzusichern
- Firmen geben immer mehr Geld aus für „gefühlte IT Sicherheit“
- Wer kann die IT Kosten rechtfertigen? Firewall, gefühlt eher die Teuren, doch warum? Gefühlt besser?
- Sicherheit ist sehr subjektiv, wir glauben wir sind sicher…

DIE GLOBALISIERUNG UND VERNETZTE WELT

- Fluch und Segen zugleich, nur wir müssen uns anpassen
- Wir müssen unseren Kindern erklären, dass der “liebe Junge“ aus Fortnite evtl. ein älterer Mann/Frau/Diverses sein kann und nicht nur Gutes im Schilde führt.
- Wir müssen den Kindern erklären, dass sie nicht alles installieren sollen/dürfen, nicht jeden Link anklicken dürfen.

DIE HERAUSFORDERUNG

- Die Technologie hat uns überrannt und wird zur echten Gefahr.
- Früher konnte man sich bequem abschotten, Firewall zu, AV an und alles war gut.
- Heute müssen Mitarbeiter sensibilisiert werden, neue Firewalls wurden kreiert, wir befinden uns mitten im Cyberkrieg
- Es ist nicht auszuschließen, dass die sog. Bots irgendwann selbstständig agieren, sobald KI die Angriffsvektoren erreicht hat.

IMMER NEUE ANGRIFFE

- Weltweit hat sich mittlerweile rumgesprochen, dass die G8 Nationen über extrem viel Kapital und Ressourcen verfügen.
- Die typische Flüchtlingswelle ist bereits angerollt.
- Es folgen die Angriffswellen der Cyberwelt.
- Ein Teenager aus Afrika, Südamerika oder anderswo, kann durch einen einfachen Angriff (Verschlüsselungstrojaner) mehrere hundert bis tausend Euro erlangen. Rosige Aussichten für ärmere Länder, die meisten G8 Staatsbürger interessiert Cybersicherheit nicht.
- Der Prinz aus Nigeria hat leider immer noch Erfolg.

WER GREIFT UNS AN?

- Automatisierte Angriffe
- Staaten bzw. deren Geheimdienste
- Aktivisten
- Scriptkiddies
- Professionelle Hacker im Auftrag
- Cyberkriminelle
- die sog. IoT Geräte bei mangelnder Absicherung
- z.B. Smart TV, Alexa oder Siri (ziemlich sicher)

WARUM WERDEN WIR ANGEGRIFFEN?

- Meistens geht es ums Geld
- Manchmal um Aktivismus (ethische Gründe , z.B. Nestlè, BP o.ä zu sabotieren)
- Weil es geht

WARUM AV ALLEINE NICHT REICHT

- 250.000 neue Viren am Tag
- Erkennungsrate guter AV bei 99 %
- 1% geht durch - am TAG
- Zeroday Exploits werden nicht erkannt

AV UND FIREWALL REICHT DOCH AUS

- Im Prinzip ja, wenn Sie sicherstellen können, dass:
  - der gesamte eingehende und ausgehende Netzwerkverkehr über die Firewalls läuft
  - Ihr Scanner mindestens 99% erkennt
  - die Nutzer nichts installieren können
  - Makros deaktiviert sind
  - alle Systeme auf dem neusten Patchstand sind
  - Sie ein 100%ig funktionierendes Backup haben und dieses regelmäßig testen.

WAS HILFT

- Regeln Sie folgende Themen:
  - Zutritt – nur Berechtigte haben Zutritt
  - Zugang - nur Berechtigte haben Zugang
  - Zugriff - nur Berechtigte haben Zugriff
  - Monitoring - sehen Sie was im Netzwerk los ist
  - Backup und Recovery: Ihre IT Lebensversicherung

UNSER VORSCHLAG

- Analysieren Sie Ihre „Kronjuwelen“: welche Prozesse benötigt Ihr Unternehmen, Ihre Behörde um zu „funktionieren“ (Notbetrieb)?
- Analysieren Sie das Risiko: was kann passieren und wie lange benötigt ein Angreifer (Time to compromise)?
- Treffen Sie Maßnahmen (ISO Controls, Grundschutz, Vds…)!

ZU STELLENDE FRAGEN

- Wissen wir wer Zugriff, Zugang und Zutritt hat?
- Wissen wir was in unserem Netzwerk los ist?
- Kennen wir ALLE Patchstände?
- Kennen wir alle Berechtigungen der einzelnen User?
- Kennen wir alle im Netzwerk befindlichen Geräte?
- Sind alle kritischen Systeme überwacht?
- Sind alle kritischen Systeme im Backup und Notfallprozess?
- Sind Makros per Standard deaktiviert?

WIE ICH ALS „MARKETINGAGENTUR“ UNTERNEHMEN HACKE..

- Seriöses Anschreiben, (bestenfalls vorhandene Agentur nehmen, Adler o.ä..)
  USB Stick unglaublich günstig anpreisen, nur für Sie, nur heute… Stick kostenlos behalten? Stick anschliessen und Bestellformular ausfüllen, die Sticks können garantiert behalten werden!!
- Anschreiben auf deren Papier/mit deren Logo…
- USB Sticks 64 GB und 128 GB beilegen..

SICHERHEIT GEHT VOR..

- Für die ersten Reihen habe ich Schutzhelme und Schutzbrillen vorbereitet..
- Manchmal geht das ins Auge…
- Der Rest bitte „Ducken wenn möglich“…

LIVE HACK USB WEITWURF

- USB Wurf, per Hand (wird schon eng bei Gegenwind)
- USB Abwurf mittels Zwille (Sieht doch schon deutlich besser aus)
- USB Abwurf mittels Drohne (denke das ist schon fast perfekt)

KURZE SCHADENSMELDUNG UNTER DEN ZUSCHAUERN

- Was glauben Sie, was würden Ihre Mitarbeiter (M/W/D) mit den Sticks anstellen?
- Hand aufs Herz, einer landet

WARUM ZUGANG WICHTIG IST

- If the light turns green, it‘s a hacked Maschine

- https://shop.hak5.org/collections/physical-access/products/bash-bunny

WIE LEICHT IST DER ZUGANG ZU ERHALTEN ?

- Wer kann 10 Sekunden einen Knopf gedrückt halten ?
- Herzlichen Glückwunsch, Sie können nun RFID Karten „Kopieren“..

- https://shop.hak5.org/products/keysy

WIE LEICHT IST DER ZUGANG ZU ERHALTEN ?

WUSSTEN SIE SCHON DASS…

- Manche Switch Hersteller „unterwegs abgefangen“ werden?
- Manche Tastaturen „Elefanten“ sind?
- Auch Ihr Monitor Sie überwachen kann?

- https://www.amazon.de/AirDrive-Forensisches-Keyloggerkabel-Hardwarekeylogger-Verlängerungskabel/dp/B07DCCBBHT/ref=sr_1_8?__mk_de_DE=ÅMÅŽÕÑ&crid=2H8FSML98P4C1&keywords=keygrabber+usb&qid=1556023584&s=gateway&sprefix=Key+grabber%2Caps%2C311&sr=8-8

- https://www.amazon.de/VideoLogger-VideoGhost-VGA-2GB-Black/dp/B0076FIIH4/ref=sr_1_1?__mk_de_DE=ÅMÅŽÕÑ&keywords=Keygrabber+vga&qid=1556024755&s=computers&sr=1-1-catcorr

- https://shop.hak5.org/products/keysy

SELBST „HACKER“ WERDEN ?

- Suchmaschinen für erste „Versuche“
- Google
- Exel-Dateien: **filetype:xl**
- Word-Dateien: **filetype:doc**
- PDF-Dateien: **filetype:pdf**
- Shodan.io für IoT Geräte
- Kameras aus Deutschland http://www.insecam.org/en/bycountry/DE/

- https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/free-ransomware-available-dark-web/