netidee PROJEKTE

Safing

Endbericht | Call 11 | Projekt ID 1638

Inhalt

1 Einleitung 3

2 Projektübersicht 3

3 Projektbeschreibung 4

3.1 Application Firewall - Portmaster 4

3.2 Safing Network - Port17 6

4 Verlauf der Arbeitspakete 8

4.1 Arbeitspaket 1 - < *Projektsteuerung und Dokumentation* > 8

4.2 Arbeitspaket 2 - < *CORE – Grundlagen* > 8

4.3 Arbeitspaket 3 - < *CORE – Application Firewall* > 9

4.4 Arbeitspaket 4 - < *CORE – Safing Network*> 9

4.5 Arbeitspaket 5 - < *CORE – Porting*> 9

4.6 Arbeitspaket 6 - < *UI – Concept & Validation*> 9

4.7 Arbeitspaket 7 - < *UI – Implementation*> 9

4.8 Arbeitspaket 8 - < *UI – Porting*> 10

4.9 Gesamtergebnis 10

5 Liste Projektendergebnisse 11

6 Verwertung der Projektergebnisse in der Praxis 11

7 Öffentlichkeitsarbeit/ Vernetzung 11

8 Geplante Aktivitäten nach netidee-Projektende 13

9 Anregungen für Weiterentwicklungen durch Dritte 13

1 Einleitung

Das Internet ist nicht kostenlos, wir zahlen mit unseren privaten Daten. Und wir von Safing haben es uns zur Aufgabe gemacht das zu ändern!

Mit Safing haben wir uns das Ziel gesetzt, uns Internetnutzer wieder die Kontrolle über unsere Daten zu geben.

2 Projektübersicht

Status

Nach deutlich über einem Jahr Entwicklungszeit haben wir den ersten großen Abschnitt des Safing Projektes verwirklicht: Die Core-Funktionen unserer Basis Suite sind fertig gestellt und wir können demonstrieren, dass unsere innovative Technologie das Zeug dazu hat den Markt ordentlich aufzumischen.

Team

Ende 2017 haben wir, auch durch das Netidee Open Source Camp angestoßen, begonnen unsere Ziele zu re-evaluieren. Herausgekommen sind wir mit zwei klare Entscheidungen:

1. Ein neues Business Model – Das Ziel sollen direkt Konsumenten sein keine Businesses
2. Wir brauchen mehr Kapazitäten und daraus resultiertend zwei Konsequenzen:
    - Ein neuer Mitstreiter kommt an Bord,
    - und wir gehen alle Vollzeit in das Projekt.

Wir sind jetzt also drei Privatsphäre Enthusiasten, alle drauf und dran qualitative open source Privatsphäre Lösungen für jeden einfach zugänglich zu machen.

Und weiter!

Ohne große Pausen (und einer kleinen Feier) starten wir nun mit der Weiterentwicklung durch um noch dieses Jahr eine minimal marktfähige Version (MVP) unsere Software zu veröffentlichen.

Ein großes Augenmerk legen wir hierbei darauf unsere Community weiter auszubauen und in das Projekt zu involvieren.

Als Team sind wir auch besonders froh über die sich anbahnende Inkubation bei Accent. Wir sind schon einige Schritte in der pre-Inkubation, und steigen in den nächsten Monaten voll ein.

Außerdem streben wir weitere Kooperationen an, zum Beispiel sind wir im Gespräch mit der ESA um Technologie von ihnen zu lizenzieren, mit der wir unser Netzwerk (Port17) weiter verbessern und optimieren können.

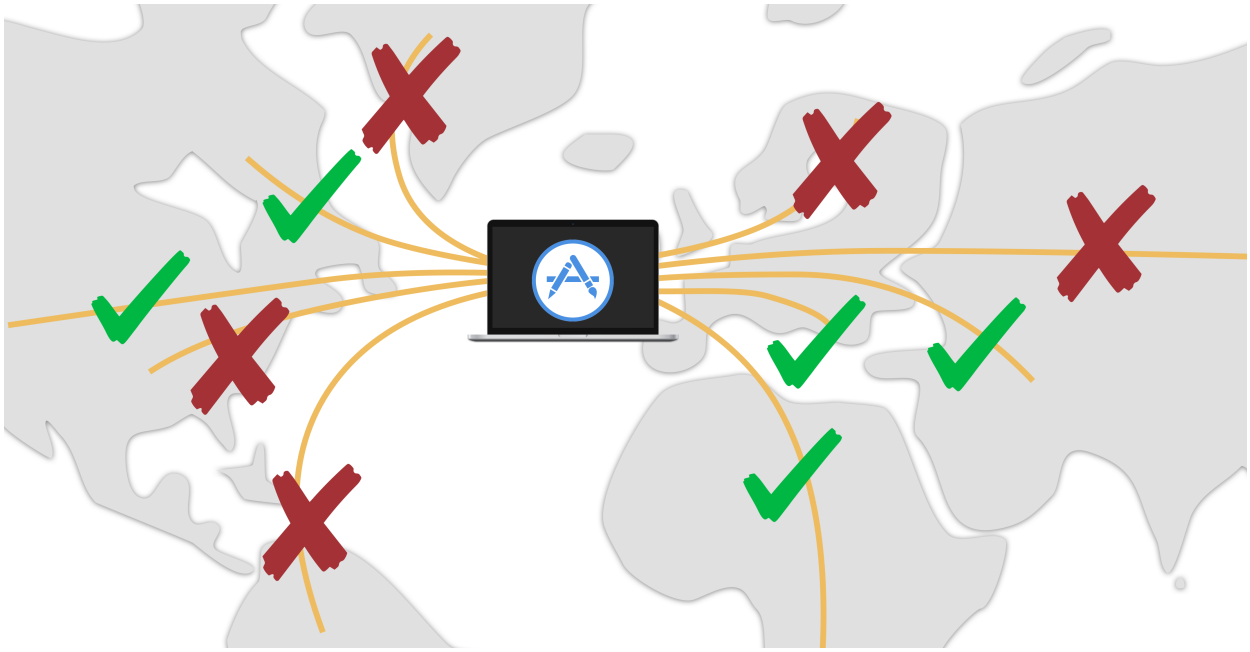
3 Projektbeschreibung

3.1 Application Firewall - Portmaster

Funktionsweise

Kurzbeschreibung

Der Portmaster ist der Türsteher des Computers ins Internet. Er prüft welches Programm sich wohin verbinden möchte und lässt nur gewünschte Verbindungen zu um das Verschicken von persönlichen Daten zu verhindern. Dabei verwendet er Verhaltensprofile der Applikationen um Entscheidungen zu treffen.



Das Resultat:

- Der Nutzer ist den Programmen die er verwendet nicht mehr hilflos ausgeliefert
- Werbung und Tracker werden in Anwendungen geblockt
- Anwendungen werden eingeschränkt, sodass sie meine persönlichen Daten nicht weiter verschicken können

In der Tiefe

Im Kern ist der Portmaster eine Firewall, die jedoch Verbindungen auf einer höheren Ebene betrachtet. Anstatt Verbindungen nur als IP-, und Port-Paar zu sehen, werden Applikation und Ziel-Domain betrachtet. Dies erlaubt es, viel feinere Kontrolle über ein-, und vor allem ausgehende Verbindungen zu erlangen.

Weiters verwendet der Portmaster “Sicherheits-Level” um dem Nutzer in einfachster Weise zu ermöglichen, die Software an aktuelle Bedürfnisse anzupassen. Diese Level werden auch von der Software selbst verändert – sofern dies nötig ist – um dem Nutzer in einer neuen oder veränderten Umgebung ausreichend Schutz zu bieten.

Die Sicherheits-Level sind:

- **Dynamic**: Für Orte, denen der Nutzer vertraut und keine Gefahren für die Privatsphäre zu erwarten sind.
- **Secure**: Für nicht unbedingt vertrauenswürdige Orte, wie etwa einem Café. In diesem Modus werden stärkere Maßnahmen gesetzt, die womöglich die Nutzung mancher Programme einschränkt.
- **Fortress**: Für den Notfall; um alle verfügbaren Maßnahmen zu aktivieren. Dieser Level wird manche Programme in ihrer Funktion einschränken und ist nur für den temporären Einsatz gedacht.

Mit diesem Stufen-Ansatz erhalten Nutzer bessere Kontrolle über ihr Privatsphäre und können auch angemessen auf eine “feindliche Umgebung” reagieren.

Verhaltensprofile ermöglichen dem Nutzer einen einfachen Weg das Verhalten eins Programmes zu definieren, ohne über die technischen Hintergründe der Netzwerktechnik Bescheid zu wissen.

Diese Profile definieren ob und wie – also auf welcher Art und Weise – Applikationen sich mit dem Internet verbinden dürfen. Profile werden Applikationen anhand ihres Datei-Pfades im System zugewiesen.

Alle Möglichkeiten der Profile werden im User Interface entsprechen erklärt. Hier wollen wir speziell auf die Optionen eingehen, mit denen ein Profil markiert werden kann. Diese Optionen erlauben es dem Nutzer mit wenigen Klicks das Verhalten einer Applikation zu definieren:

- Ausführender Nutzer
  - System: Wird dieses Programm nur vom System verwendet?
  - Admin: Darf dieses Programm nur von Administratoren verwendet werden?
  - User: Ist dieses Programm für den Nutzer gedacht?
- Netzwerk-Bereiche
  - Internet: Darf sich diese Applikation mit dem Internet verbinden?
  - LocalNet: Darf sich diese Applikation mit dem lokalen Netzwerk verbinden?
- Netzwerk-Ziele
  - Strict: Soll sich diese Applikation nur mit zugehörigen Servern verbinden?
  - Gateway: Bestimmt der Nutzer die Zielserver der Applikation?
  - Service: Stellt diese Applikation ein Netzwerkservice zur Verfügung?

Ein besonderes Augenmerk ist auf die Option “Strict” zu legen. Mit dieser Option versucht der Portmaster eine Korrelation bzw. Zugehörigkeit zwischen dem Programm und dem Zielserver zu erkennen um ohne jegliche weitere Konfiguration eine Applikation auf die ihm zugehörigen Server zu beschränken.

Diese Profile ermöglichen es dem Nutzer ganz einfach Programme in die Schranken zu weisen und seine Privatsphäre zu schützen. Zur weiteren leichteren Handhabung werden diese Profile zukünftig von einer von der Community verwalteten Plattform geladen.

Status

Der Portmaster befindet sich in der Tech-Preview bzw. Early-Alpha Phase. In dieser Phase sind alle Features für das MVP (minimal viable product) bereits fertig, jedoch fehlt der Feinschliff der Kernkomponenten sowie nutzerseitige Hilfestellungen (als Teil der Software)

Potential

Mit seiner einzigartigen Funktionsweise wird der Portmaster schon bald Menschen aus aller Welt davor schützen, dass ihre persönliche Daten abfließen und sie im Internet auf Schritt und Tritt überwacht werden.

Besonders auch mit der DSGVO sehen wir Potential. Der Portmaster kann beim Anwender sicherstellen, dass Applikationen mit denen Kundendaten verwaltet werden noch besser geschützt sind.

Wir wollen diese Technologie auf immer mehr Plattformen verfügbar machen. Derzeit haben wir uns auf Desktops konzentriert, aber gerade auch auf mobilen Endgeräten ist Privatsphäre viel wichtiger geworden.

3.2 Safing Network - Port17

Funktionsweise

Kurzbeschreibung

Mit Port17 stellen wir sicher, dass deine Daten auch auf dem Transport zu ihrem Ziel sicher sind. Dabei schützen wir unsere Nutzer nicht nur davor, dass ihre versendeten Daten geschützt sind, sondern auch ihre Metadaten. Wer Port17 verwendet kann beim Surfen im Internet ein bisher unerreichtes Maß an Privatsphäre genießen.

Dieses Netzwerk ist einzigartig, weil mit jeder Verbindung ins Internet ein eigener Pfad in diesem Netzwerk gebaut wird. Port17 kombiniert dabei den Zielort und den nächsten Server unseres Netzwerkes, um die Verbindung nur so kurz wie möglich dem ungeschützten Internet auszusetzen.

Das Resultat:

- Aus Sicht des Internets bist du an mehreren Orten Gleichzeitig
- Der Zielserver (zB.: facebook.com) weiß nicht wo du bist
- Internet Provider (zB.: A1, UPC usw.) sehen nicht wohin sich der Nutzer verbindet
- Sämtliche Daten sind geschützt, ich kann bedenkenlos in öffentlichen Netzwerken (Hotspots) surfen

In der Tiefe

Port17 ist ein Mesh-Netzwerk, das sich zwar dynamisch aufbaut, aber die Verbindungen zwischen den einzelnen Knoten sind recht statisch. Jeder diese Knotenpunkte teilt mit den anderen Informationen über sich selbst, sodass jeder über jeden anderen Knoten Bescheid weiß.

Aus Sicht des Nutzers fühlt sich Port17 ähnlich an wie ein VPN-Service. Man aktiviert es und surft ab nun über gesicherte Leitungen im Netz. Der Unterschied ist aber beträchtlich: Bei einem VPN wird lediglich eine sichere Verbindung zu einem Server des Anbieters aufgebaut. Von dort nehmen die Verbindungen ins Internet wieder lange Wege durch ungeschützte Netzwerke auf sich.

Anders ist das bei Port17. Da bekommt jede Verbindung zu einem Zielserver eine eigene verschlüsselte Leitung und wird innerhalb des Port17 Netzwerkes so nah wie möglich zum Zielserver transportiert. Dadurch erreicht der Nutzer eine noch nie dagewesene Privatsphäre beim Surfen im Internet.

Verbindungen innerhalb Port17 sind mehrfach verschlüsselt (onion encryption). Dies hat zur Folge, dass die Software, die auf dem Rechner des Nutzers läuft, über das Netzwerk Bescheid wissen muss um die Route auszuwählen und die Verschlüsselung korrekt aufzusetzen.

Status

Port17 befindet sich in der Tech-Preview bzw. Early-Alpha Phase. In dieser Phase sind alle Features für das MVP (minimal viable Product) bereits fertig, jedoch fehlt der Feinschliff der Kernkomponenten sowie nutzerseitige Hilfestellungen (als Teil der Software) zur Nutzung.

Im Zuge der Beta wird es auch erstmals ein für Nutzer verfügbares Netzwerk geben.

Potential

Port17 steht mit seinem Potential noch sehr am Anfang. Die entwickelte Technologie kann in mehreren Bereichen angewendet werden, wovon die Privatsphäre beim Surfen erst der Anfang ist.

4 Verlauf der Arbeitspakete

4.1 Arbeitspaket 1 - *< Projektsteuerung und Dokumentation >*

Neben den organisatorischen Arbeiten ging es hier vor allem um die Dokumentation der Software, sowie das Erstellen von Konzepten.

Die Projektlaufzeit hat sich durch mehrere Faktoren erheblich verlängert:

- Umfang der Implementierungsarbeiten wurden unterschätzt
- Anfangs war der Fokus noch nicht so gegeben und es kam vor, dass man sich in Details verloren hat, die erst später dran waren.
- Die nebenläufige Arbeitsstelle hat zeitweise sämtliche Ressourcen beansprucht.
- Der jedoch größte Faktor war, dass es unheimlich viel Zeit gekostet hat, ein Business Model zu entwerfen und dazu einen Business Plan zu schreiben, der jeder Kritik standhält.

In Zukunft soll uns eine bessere Planung Abweichungen früher aufzeigen um besser darauf zu reagieren.

4.2 Arbeitspaket 2 - *< CORE – Grundlagen >*

Die Grundlagen des Systems sind allesamt fertig und werden aktiv im Projekt verwendet. Durch das einsetzen in den anderen Software-Teilen wurde klar, dass manche Teile davon aber noch verbessert werden müssen.

4.3 Arbeitspaket 3 - *< CORE – Application Firewall >*

Die Application Firewall – der Portmaster – wurde von Grund auf implementiert. Die Herausforderung war die Schnittstelle zum Betriebssystem, da es für diesen Anwendungsfall keinen vorgesehenen Eingriffspunkt gibt, sondern es müssen aus verschiedenen Interaktionen mit dem System die einzelnen Informationen zusammengetragen werden um die gewünschte Integration zu erreichen. In dieser Hinsicht war und ist vor allem die Stabilität dieser Integration die größte Herausforderung.

4.4 Arbeitspaket 4 - *< CORE – Safing Network>*

Das Safing Netzwerk ist das große Arbeitspaket des nächsten Meilensteins, die Arbeiten daran haben bereits begonnen.

Das Safing Netzwerk – Port17 – ist die komplexeste Komponente des Systems.

4.5 Arbeitspaket 5 - *< CORE – Porting>*

Hierbei ging es darum den Core – Portmaster und Port17 – auf Windows und MacOS zu portieren.

Windows: Die Portierung hier lief wie erwartet – mit ein paar kleinen Herausforderungen – sehr gut ab.

MacOS: Bereits beim letzten Bericht hat es zur Portierung zu MacOS neue Entwicklungen gegeben. Bei weiterer Prüfung hat sich zwar die Machbarkeit bestätigt, jedoch ist das benötigte Zeitausmaß explodiert, sodass sich die Portierung in diesem Projekt leider als unmöglich herausgestellt hat.

Grund dafür ist die Art und Weise wie Apple sein Betriebssystem (nicht) zugänglich macht und daher der Betriebssystem-Kern durch eine Erweiterung ergänzt werden muss. Diese Komplexität und Zeitaufwand war am Anfang nicht absehbar.

4.6 Arbeitspaket 6 - *< UI – Concept & Validation>*

Die Konzeptionierung des UI war ein spannender Prozess. Im Laufe der Arbeiten haben wir uns immer wieder kleinen Herausforderungen stellen müssen, um ein Nutzerinterface zu gestalten, dass unseren Anforderungen entspricht: So intuitiv wie möglich zu bedienen und vor allem zu verstehen, ohne Abstriche bei der Funktionalität hinzunehmen.

4.7 Arbeitspaket 7 - *< UI – Implementation>*

Die Implementierung des User Interfaces hat mehr Zeit in Anspruch genommen als geplant. So konnten wir leider keine zusätzlichen Ansichten mehr einbauen – trotzdem finden wir – zeigt das User Interface sehr schön die Komplexität und Stärken des Portmasters.

4.8 Arbeitspaket 8 - *< UI – Porting>*

Die Portierung der UI stellte – neben ein paar Unannehmlichkeiten – keine Herausforderung dar.

4.9 Gesamtergebnis

In allem waren diese letzten 1½ Jahre eine sehr arbeits- und ergebnisreiche Zeit. Unsere Vision – allen Menschen mehr Privatsphäre im Internet zu geben – langsam in eine Form zu gießen ist etwas ganz Besonderes, es wird dabei immer spannender, je näher wir unserem Ziel kommen.

Um diese tolle Zeit etwas zu quantifizieren, hab wir uns von einem tollen Tool (scc) folgende Tabelle errechnen lassen, die sehr schön zeigt, wie ertragreich diese Zeit war – und wie viel wir in dieser kurzen Zeit geschafft haben:

```
-------------------------------------------------------------------------------
Language                 Files     Lines     Code  Comments   Blanks Complexity
-------------------------------------------------------------------------------
Go                         269     31315    23982      2900     4433       4313
Markdown                    36      1632     1119         0      513          0
HTML                        31       827      770        10       47          0
JavaScript                  30      4033     3629       177      227        222
YAML                        12       426      325        59       42         10
SVG                         12       600      571         8       21          0
Sass                         9       450      383         0       67          0
Shell                        3        64       45         4       15         11
XML                          3        34       34         0        0          0
C Header                     2       372      268        65       39          9
Ruby                         2       112       98         0       14         11
JSON                         2        82       82         0        0          0
CSS                          2       233      191         2       40          0
BASH                         1        39       29         3        7          5
PHP                          1         8        6         0        2          0
C                            1        88       70         2       16         16
-------------------------------------------------------------------------------
Total                      416     40315    31602      3230     5483       4597
-------------------------------------------------------------------------------
Estimated Cost to Develop $1,014,601
Estimated Schedule Effort 15.427058 months
Estimated People Required 7.790533
-------------------------------------------------------------------------------
```

Wir sind uns nicht sicher, wie sehr man diesen Einschätzungen vertrauen kann, doch veranschaulichen diese aus unserer Sicht gut, wie viel Zeit und Energie wir bisher in das Projekt hineingesteckt haben.

5 Liste Projektendergebnisse

1	**Projektendbericht**	CC BY-SA	https://www.netidee.at/safing
2	**Entwickler-Dokumentation**	CC BY-SA	https://docs.safing.io
3	**Anwender-Dokumentation**	CC BY-SA	https://docs.safing.io
4	**Veröffentlichungsfähiger Einseiter**	CC BY-SA	https://www.netidee.at/safing
5	**Safing Software -** Betriebssystemübergreifende Elemente - Das Gesamtpaket der im Rahmen des Projektes erstellten Software	GPL / APGL	github.com/Safing
6	**Safing Software** – Windows-spezifische Elemente	GPL / APGL	github.com/Safing
7	**Safing Software** – Mac-spezifische Elemente	GPL / APGL	github.com/Safing
8	**Safing Software** – Linux-spezifische Elemente	GPL / APGL	github.com/Safing

6 Verwertung der Projektergebnisse in der Praxis

In der derzeitigen Fassung wurde die Software noch nicht von Dritten verwendet. Die Arbeiten am letzten Feinschliff beginnen nun und warten schon sehnsüchtig auf Feedback unserer ersten Alpha-Tester.

7 Öffentlichkeitsarbeit/ Vernetzung

Unser Plan in der Öffentlichkeitsarbeit hat zwei Stufen: zuerst bauen wir eine Kerngruppe von Privatshäre-Enthusiasten, mit denen wir unsere Produkte an allen Ecken und Kanten schleifen, glätten & verbessern. Erst dann wollen wir an die breite Öffentlichkeit treten.

Mit der ersten Stufe haben wir bereits begonnen.

Die Kerngruppe (der “Tribe”)

Das Thema Privatsphäre ist weitreichend und benötigt aufgrund der Komplexität der verfügbaren Lösungen oftmals Unterstützung. Daher gibt es im Internet schon einige etablierte Communities, die sich darüber austauschen. Wir haben angefangen uns mit diesen Gruppen in Verbindung zu setzen, zu teilen was wir wissen und einen positiven

Einfluss mitzubringen noch bevor unser Produkt verbreitungsfähig ist. Aus diesen Gruppen heraus starten wir den Kern der Safing Community. Das Ziel mit dieser Kerngruppe – der “Tribe” – ist es, unsere Produkte zu iterieren und weiter zu entwickeln.

Die etablierte Privatsphäre-Community stellt folgende Bedingungen an Software Tools:

- Sie muss Open Source seine
- Sie soll ein klares Geschäftsmodell haben
- Sie darf selbst keine Daten sammeln

Wir haben diese drei Punkte voll in unseren Überlegungen integriert: Unsere Produkte sind aus Überzeugung Open Source, wir haben ein klares Geschäftsmodell und wir bauen aktiv an einer Community um Nutzer-Feedback auf freiwilliger Basis zu bekommen – anstatt diese über die Applikation abzusaugen.

Der Ort an dem wir unsere Öffentlichkeitsarbeit bündeln ist unser Safing Community Hub, wo wir unsere Haupt-Kommunikationswege erklären. Dabei bildet unser Discourse Forum unser zentrales Rückgrat – dort wollen wir die Community bauen und betreuen.

In der Öffentlichkeitsarbeit ist es sehr wichtig Vertrauen aufzubauen. Deshalb haben wir auch unsere Werte zu einem zentralen Punkt auf unserer Homepage gemacht: darauf beschreiben wir, warum Open Source und ethisch gute Finanzierungen für uns so wichtig sind. Wir legen auch klar offen woher unsere Finanzierungen bisher kamen. Die Netidee steht dort auch als großer Finanzierender dabei.

Bei unserem letzten Website-Revamp war unsere Priorität klarer zu kommunizieren. Die oben erwähnten Seiten waren ein Teil davon, aber vor allem wollten wir unsere Idee und unsere Produkte verständlicher und zugänglicher machen. Deshalb ist die Homepage jetzt mit kürzeren und leichter verständlichen Texten bestückt. Um aber auch den Wissensdrang von technisch versierten Besuchern zu stillen, haben wir eine eigene Technologie-Seite erstellt, in der wir viele technische Details erklären.

Die allgemeine Öffentlichkeit

Erst wenn die wichtigsten Anpassungen durch sind und unsere Suite tadellos funktioniert, werden wir den Push in die allgemeine Öffentlichkeit machen. Unser Ziel dabei ist es, jedem die Möglichkeit zu geben, Privatsphäre im Internet auf eine einfache Art und Weise zu genießen.

Neben den Herausforderungen, die durch die Skalierung unserer Produkte entstehen werden, gilt es auch, „Awareness“ zum Thema Privatsphäre zu bilden. Privatsphäre sagt zwar jedem schnell etwas – wir sind auch alle betroffen – doch das Ausmaß der Invasion in das tägliche Leben ist den meisten Menschen nicht ganz klar.

8 Geplante Aktivitäten nach netidee-Projektende

Wir wollen die Performance des Portmasters - der Applikation Firewall - unbedingt optimieren. Wir „genießen“ gerade die hohe Performance, die Desktop-Betriebssysteme bieten, wollen aber die Anwendung so effizient wie möglich machen. Gerade auch weil jegliche Optimierung essenziell für eine Portierung auf leistungsschwächere oder akkubetriebene Geräte - wie zum Beispiel Mobiltelefone - notwendig ist.

Um einen bestmöglichen Schutz zu gewährleisten ist die richtige Konfiguration der Anwendung wichtig, deshalb übernimmt der Protmaster das im Normalbetrieb selbst. Sollte der Nutzer selbstständig eine Änderung vornehmen wollen besteht immer die Gefahr einer Fehleinstellung, womit die Privatsphäre gefährdet wäre. Daher planen wir das UI weiter zu verbessern und gerade für die Fehlerbehebung einen Assistenten zu bauen, der Nutzern dabei hilft Probleme schnell und risikofrei zu beheben.

9 Anregungen für Weiterentwicklungen durch Dritte

Beide unserer Projektteile geben ganz eigene Möglichkeiten der Weiterentwicklung:

Für den Portmaster (die Applikation Firewall) bietet sich eine Portierung auf eine mobile Plattform sehr an. Wir denken auch an, auf Unternehmen zuzugehen und ihnen diese Option zu präsentieren.

Auch gerade in Bezug auf die DSGVO sind Projekte mit einem Fokus auf IOT und Serversicherheit spannend.

Unser Netzwerk (Port17) kann mit noch etwas Arbeit gut in mobilen Bereichen angewendet werden. Drei interessante Möglichkeiten sehen wir heute schon:

- Wir schaffen bei niedrigen datenraten maximale Geschwindigkeiten zu liefern
- Verbindungen können wieder aufgenommen werden, nachdem sie unterbrochen wurden
- Es können mehrere Internetverbindungen gleichzeitig genutzt werden

Privatsphäre ist uns ein großes Anliegen, und suchen mit großem Interesse nach Projekten denen es auch ein Anliegen ist gemeinsam an einer besseren Zukunft zu bauen.