

# Usermanual for ITSecX

Erik Brändli

21.05.2015

Version	Name	Datum	Status	Unterschrift
v 1.0.1us	Erik	18.06.2015	unstable	
v 1.0.1ps	Erik	18.06.2015	pretty-stable	
v 1.0.1s	Erik	19.06.2015	stable	
v 1.0.1	Hüseyin Bozkurt	21.06.2015	Freigeben	

# 1 Inhaltsverzeichnis

## Contents

1	Inhaltsverzeichnis	2
2	Einleitung	4
2.1	Autoren und Mitwirkende	4
2.2	Autoren und Editoren	4
2.3	Einsatzgebiet	4
3	Vorbereitung des Produktes	5
3.1	Vorausgesetztes	5
3.2	Erstellen eines tcpdump-services	5
3.3	Erweiterungen	5
4	Installation des Produktes	5
5	Inbetriebnahme	5
6	Funktionen	6
6.1	Datei	6
6.1.1	IP Settings	6
6.1.2	Import → Settings	6
6.1.3	Export → Settings	6
6.1.4	Verbindung → verbinden	7
6.1.5	Verbindung → trennen	7
6.2	Tools	8
6.2.1	Scanner → nmap	8
6.2.2	Sniffing → tcpdump → start/stop	8
6.2.3	Direct Command	9
6.3	Files	10
6.3.1	View File	10
6.3.2	View tcpdump	11
6.3.3	View tcpdump → Download	11
6.4	Window	12
6.4.1	Set Fontcolor	12
6.4.2	Set bgcolor	12
6.4.3	Clear	12
7	Schritt-für-Schritt Beispiel	13

8	Rechtliche Hinweise	15
8.1	Haftungsausschluss . . . . .	15
8.2	Lizenz . . . . .	15
8.3	Urheberrechte . . . . .	15

## 2 Einleitung

EditierenITSecX ist die Abkürzung für "IT - Security - Extreme". ITSecX lässt sich mit dem von uns zur Verfügung gestellten Devices verbinden.

Die interne Syntax ist C # . Das Hauptziel des Projektes ist es zu zeigen, wie einfach man Daten Abfangen und auswerten kann und Amateur Pen-Testern die Möglichkeit zu geben, schnell dynamisch an Ziele gelangen. Es ist auch möglich aus der zur Verfügung gestellten Software weit mehr rauszuholen (gegen Aufpreis).

Dieses Handbuch besteht vorrangig aus einer Funktionsreferenz, Erläuterungen zu den wichtigsten Features und weitere ergänzende Informationen.

### 2.1 Autoren und Mitwirkende

Das Projektteam bestand aus 5 Mitgliedern von denen aktuell noch 2 vorhanden sind.

- ) Erik Brändli
- ) Hüseyin Bozkurt
- ~~-) Markus Schulmeister~~
- ~~-) Arian Sayah~~
- ~~-) Raied El'beidak~~

Projektabnehmer:

- ) Michael Borko
- ) Werner Kristufek
- ) Erich Trenner
- ) Elisabeth Wildling

### 2.2 Autoren und Editoren

Folgende Personen verdienen Anerkennung dafür, dass Sie wesentlichen Inhalt zum Handbuch beigetragen haben und/oder weiterhin beitragen werden: Hüseyin Bozkurt und Erik Brändli.

Vielen Dank!

### 2.3 Einsatzgebiet

Als Einsatzgebiet sind Schulen mit IT-Ausbildung gedacht, da man dort den Schülern lehren, kann wie einfach es ist ein Netzwerk auszutricksen bzw. um zu veranschaulichen, dass Netzwerksicherheit ein wichtiger Part in unserer Welt ist.

Denn die meisten Schüler denken, dass ihre Daten sicher sind, und dass niemand mitlesen kann!

## 3 Vorbereitung des Produktes

Sollten Sie bereits unser modifiziertes "Arch Linux" besitzen können Sie dieses Kapitel überspringen.

### 3.1 Vorausgesetztes

Um das Produkt zu verwenden erwerben Sie am besten unser "Arch Linux" von unserer Seite, oder Sie installieren sich zu Ihrer Arch Linux version folgende Pakete dazu:

- ) Openssh
- ) openbsd-netcat
- ) nmap
- ) tcpdump
- ) dsiff

### 3.2 Erstellen eines tcpdump-services

Falls Sie nicht unser modifiziertes "Arch Linux" verwenden müssen Sie sich einen Service schreiben welches einen tcpdump startet auf einem von Ihnen ausgewählten Interface startet. Dieser Dump muss in eine Datei geschrieben werden, wie dies funktioniert finden sie auf der Seite von tcpdump.(<http://www.tcpdump.org/>)

### 3.3 Erweiterungen

Um folgende Dinge müssen Sie sich kümmern:

- ) Es sollte sich der Tcpdump bei Systemstart von alleine starten.
- ) Sudo befehl muss ohne Passwort erfolgen

## 4 Installation des Produktes

Führen Sie den gelieferten Installer aus um die Software zu installieren.

AxNetworks ist eine wichtige externe Komponente, damit die Software auf dem Windowsgerät läuft. Nach erfolgreicher Installation ist das Produkt voll einsatzbereit.

## 5 Inbetriebnahme

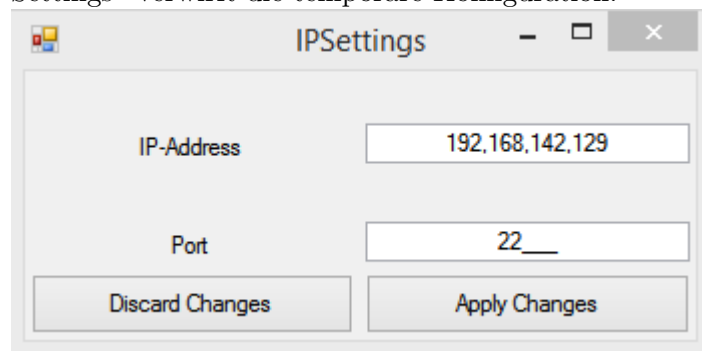
## 6 Funktionen

In diesem Kapitel werden die Funktionen der Gui erklärt bezüglich ihrer Anwendung und Auswirkung

### 6.1 Datei

#### 6.1.1 IP Settings

In "IP Settings" lässt sich festlegen zu welchem Device man sich verbinden möchte. Man findet zwei maskierte Eingabefelder wieder. Das Eingabefeld mit IP-Address nimmt die IP-Adresse(v4) vom Device entgegen und validiert ob diese IP korrekt ist. Das Feld nimmt eine bis zu 4 stellige Zahl zur Definierung des Kommunikations-Port am Device. Mit dem Knopf "Apply Settings" können Sie die Einstellungen übernehmen. "Discard Settings" verwirft die temporäre Konfiguration.



#### 6.1.2 Import → Settings

Ermöglicht das Importieren von Konfigurationen bezüglich:

- ) **Verbindung-Punkt (IP:Port)**
- ) **Authentifizierung (Username, Passwort)**

Ein OpenFileDialog öffnet sich und bittet Sie darum eine Datei auszuwählen, eine **.conf** Datei (Die Sie mit unserer Software erstellten, siehe auch Kapitel 6.1.3) Desweiteren wird die Verbindung sofort getestet um zu überprüfen ob die übergebenen Daten korrekt sind, und das Device verfügbar ist. **Dies kann in gewissen Fällen länger dauern.**

#### 6.1.3 Export → Settings

Ermöglicht das Exportieren von Konfigurationen bezüglich:

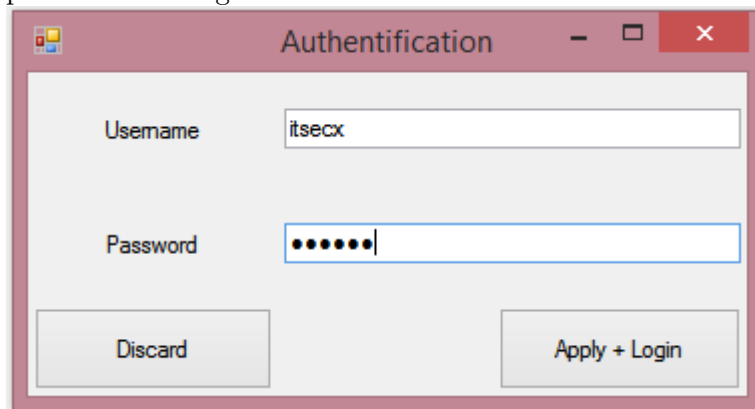
- ) **Verbindung-Punkt (IP:Port)**
- ) **Authentifizierung (Username, Passwort)**
- ) Interface-Settings (Schriftfarbe, Hintergrundfarbe, ...)

Desweiteren wird empfohlen eine Setting erst dann zu exportieren wenn die Verbindung

bereits getestet wurde. **Diese Datei enthält sensible Daten bitte schützen Sie sich selbst, indem Sie diese Datei schützen**

#### 6.1.4 Verbindung → verbinden

Über diesen Menüpunkt verbindet man sich zum Device, dafür ist jedoch erforderlich, dass Sie Ihre Daten in die Felder "Username" & "Passwort" eintragen. Danach bestätigen Sie Ihre Eingabe mit dem Button "**Apply + Login**", durch das klicken auf den Button probiert das Programm sich zu dem Device zu verbinden.



#### 6.1.5 Verbindung → trennen

Mit der Funktion trennen lässt sich die Kommunizierschnittstelle zurücksetzen, folglich sind Sie vom Device getrennt. um sich erneut zu verbinden müssen Sie alle Settings neu eingeben, oder Sie laden eine Konfiguration über Import → Settings (6.1.2)

## 6.2 Tools

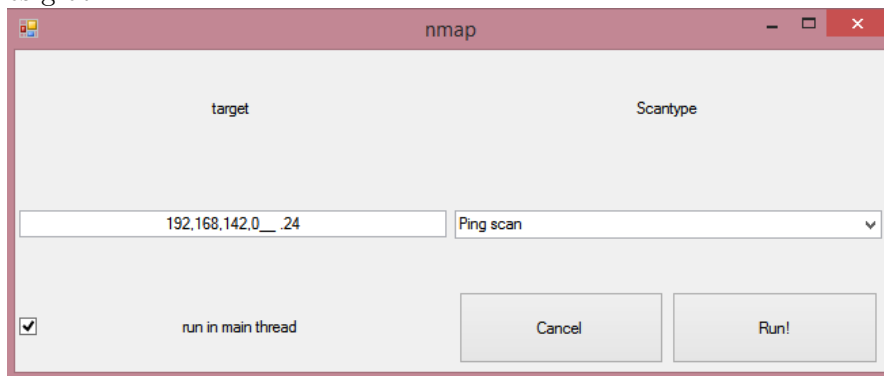
Hier befinden sich jene Tools die das Device ausführen kann, Konfigurationen für diese Tools werden automatisch geladen bzw. in einem Fenster für Sie bereit gestellt, dass sie nur mehr auswählen müssen wer & was.

### 6.2.1 Scanner → nmap

nmap ("Network Mapper") ist ein Tool womit Sie einen fremden Computer:

- ) prüfen können ob dieser Ein-/Aus-geschaltet ist
- ) schauen weleche Ports offen hat
- ) evtl. erkennen welches Betriebssystem auf diesem Computer läuft.
- ) wie weit dieser Computer entfernt ist Hier bei ist nicht die Rede von wie viele

Meter ist dieser Computer weg, sondern wieviele netzwerktechnische zwischen Punkte es gibt.



### 6.2.2 Sniffing → tcpdump → start/stop

tcpdump legt die Netwerkpakete in einem Logfile(**.pcap**) ab.

Mit der Funktion **start** wird der "Dump" in eine Datei geschrieben.

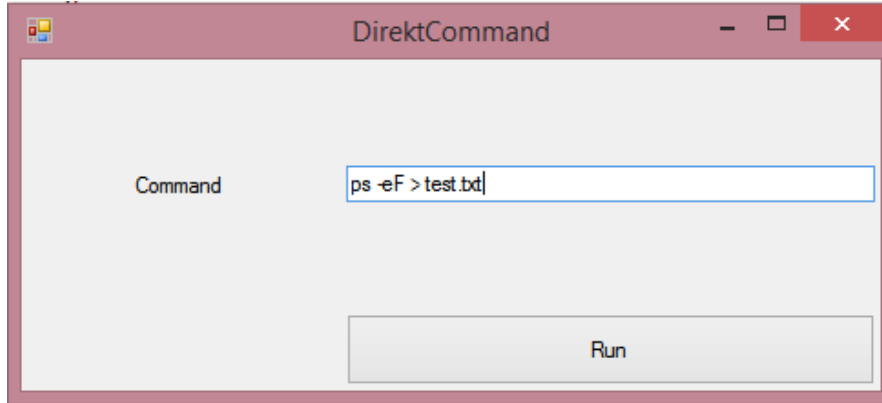
! Sollte es bereits gestartet sein, wird dieser neugestartet.

Mit der Funktion **stop** wird der "Dump" angehalten.



### 6.2.3 Direct Command

Über diese Funktion ist es möglich einen Befehl am Device auszuführen, denn evtl. möchten Sie selbst etwas auslesen oder umstellen.

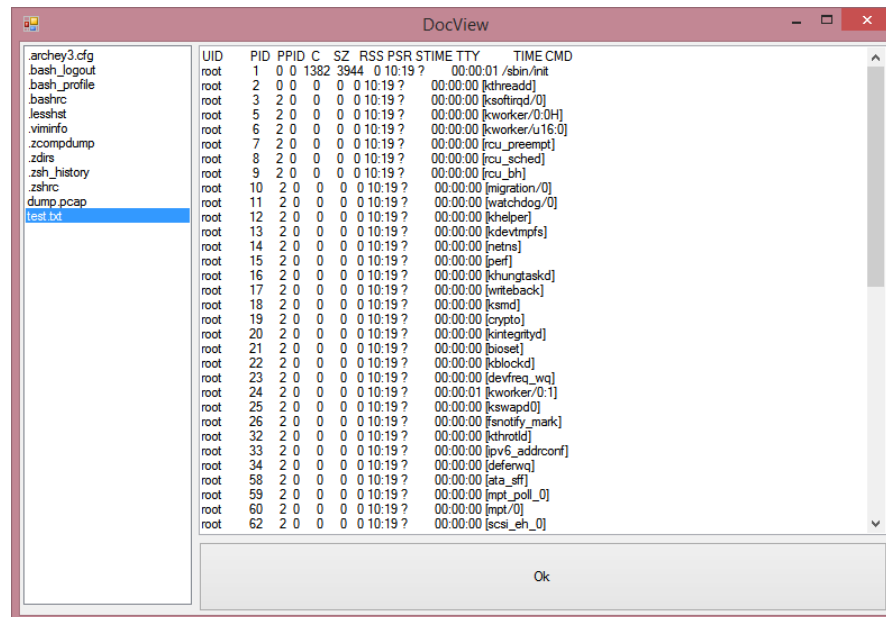


## 6.3 Files

Mit den Funktionen in diesem Menü können Sie mit den Logs und Dateien arbeiten, also diese anzeigen und herunterladen.

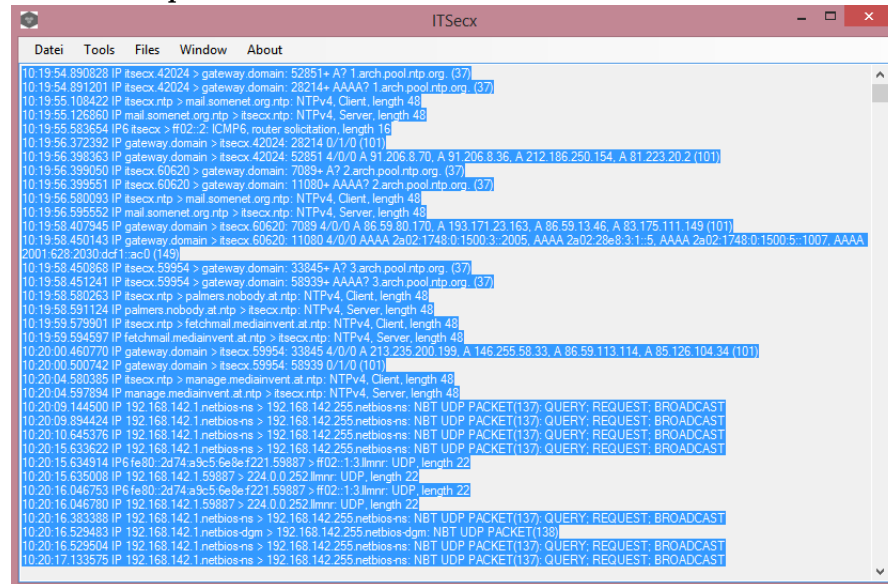
### 6.3.1 View File

Hier können Sie in dem Sie die auf der linken Seite eine Datei auswählen diese anzeigen.



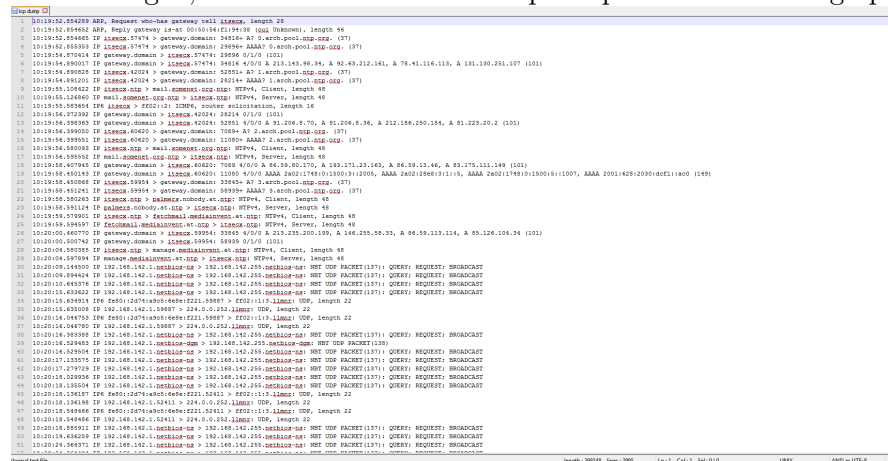
### 6.3.2 View tcpdump

Wenn Sie diese Aktion ausführen wird der aktuelle tcpdump im Hauptfenster ausgegeben. **Da diese Daten erst konvertiert werden müssen kann dies eine gewisse Zeit in anspruch nehmen!**



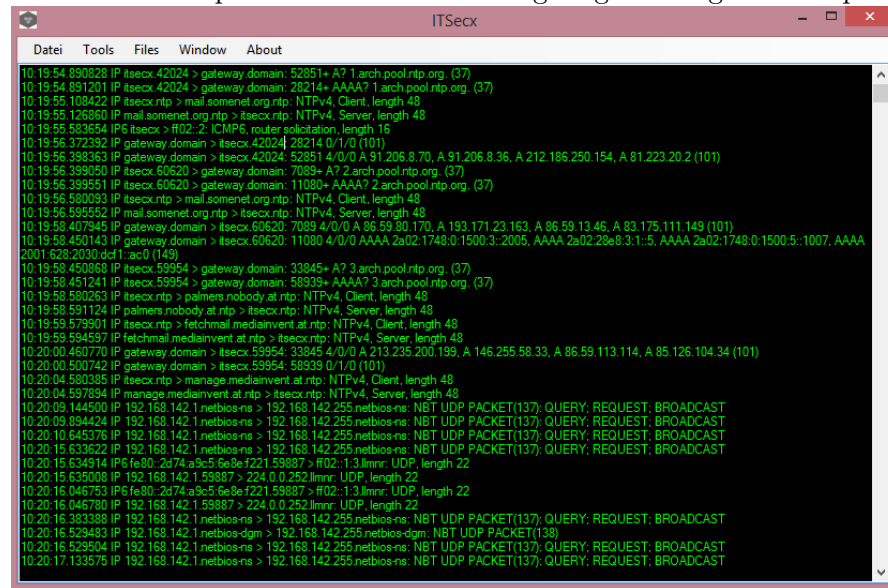
### 6.3.3 View tcpdump → Download

Sollten Sie diese Funktion auswählen kommt ein "speichern unter" Dialog diesen müssen Sie bestätigen, dann wird der aktuelle tcpdump an dieser Stelle gespeichert.



## 6.4 Window

In diesem Menüpunkt können Sie den angezeigten Ausgabetext optisch bearbeiten.



### 6.4.1 Set Fontcolor

Hier können Sie die Textfarbe wählen.

### 6.4.2 Set bgcolor

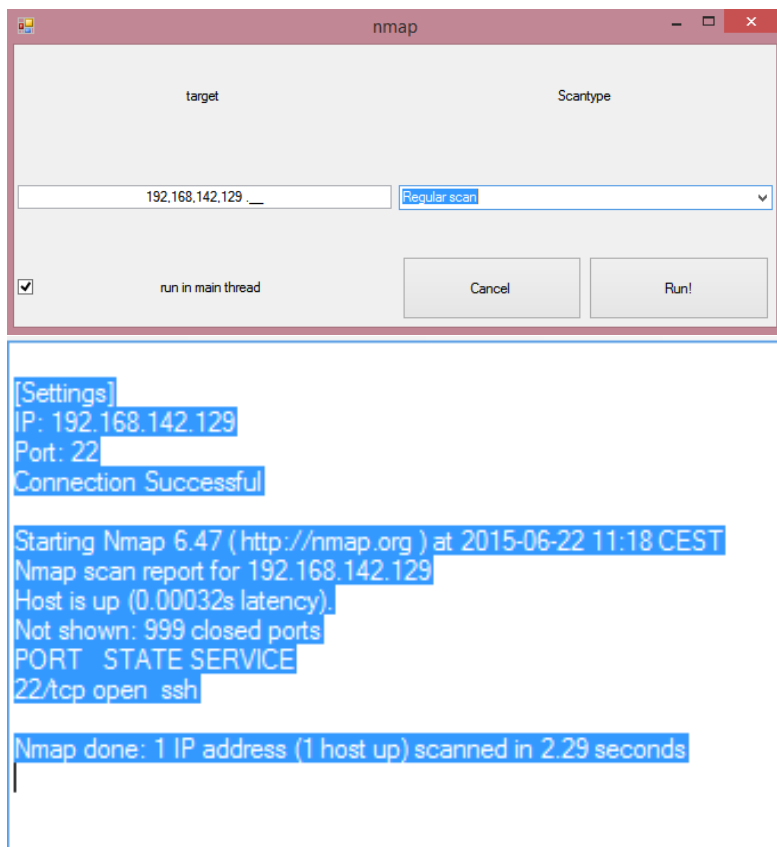
Hier können Sie die Hintergrundfarbe wählen

### 6.4.3 Clear

Mit dieser Funktion leeren Sie die Ausgabe im Hauptfenster

## 7 Schritt-für-Schritt Beispiel

The image shows two overlapping windows from the ITSecX application. The top window, titled "IPSettings", has a light gray background and contains two text input fields: "IP-Address" with the value "192.168.142.129" and "Port" with the value "22\_\_". Below these fields are two buttons: "Discard Changes" and "Apply Changes". The bottom window, titled "Authentification", has a maroon header bar and a light gray body. It contains two text input fields: "Username" with the value "itsecx" and "Password" with masked characters "••••••". Below these fields are two buttons: "Discard" and "Apply + Login". Below the "Authentification" window is a small status area with a blue border, displaying the following text: [Settings]  
IP: 192.168.142.129  
Port: 22  
Connection Successful]



## 8 Rechtliche Hinweise

### 8.1 Haftungsausschluss

Die Dokumente der ITSecX enthalten Links zu externen Webseiten. Die Inhalte der externen Webseiten sind Implementierungen und nicht im Angebot inkludiert. Die Links sind ausschließlich Verweise zu ergänzenden Informationen zu verstehen. Auf die Inhalte der verlinkten Webseiten haben wir keinen direkten Einfluss. Zum Zeitpunkt der Verlinkung waren rechtswidrige Inhalte nicht erkennbar. Falls solche Inhalte zu einem späteren Zeitpunkt bekannt werden sollten, werden die betreffenden Inhalte angepasst.

### 8.2 Lizenz

Die ITSecX möchte sich Ihnen mit einem erfolgreichem Produkt präsentieren. Das darin enthaltene geistige Eigentum wie Patente, Marken und Urheberrechte ist geschützt. Durch dieses Produkt wird keine Lizenz zur Nutzung des geistigen Eigentums der Marke ITSecX erteilt.

### 8.3 Urheberrechte

© Copyright TGM, 1200 Wien. Alle Rechte vorbehalten. Text, Bilder, Grafiken, Sound, Animationen und Videos sowie deren Anordnung auf dem ITSecX-Produkt unterliegen dem Schutz des Urheberrechts und anderer Schutzgesetze.

Es wird untersagt, den Inhalt dieses Produktes oder Teile davon, zu kommerziellen oder auch zu privaten Zwecken zu kopieren, zu verbreiten, zu verändern, auf anderen Websites zu verwenden oder Dritten zugänglich zu machen.