

1.– 4. September 2014  
in Nürnberg



# Herbstcampus

Wissenstransfer  
par excellence

## Risiko Datensicherheit

End-to-End-Verschlüsselung von Anwendungsdaten

Peter Kirchner  
Microsoft Deutschland GmbH

**Tages  
prophet**

# **RISIKO**

## **Datensicherheit**

**NSBNKPDA kennt alle ihre Geheimnisse!**

Unterschleißheim – Jüngste Studien haben ergeben, dass Ihre Daten nur noch unter Ihrem Kopfkissen sicher sind. Handeln Sie schnell!

Lesen Sie hier nicht weiter, sondern hören Sie dem

nicht weiter, sondern hören Sie dem Referenten zu. Lesen Sie hier nicht weiter, sondern hören Sie dem Referenten zu. Lesen Sie hier nicht weiter, sondern hören Sie dem Referenten zu. Lesen Sie hier nicht weiter, sondern hören Sie dem Referenten zu. Lesen Sie hier nicht weiter, sondern hören Sie dem Referenten zu.

Sie dem Referenten zu. Lesen Sie hier nicht weiter, sondern hören Sie dem Referenten zu. Lesen Sie hier nicht weiter, sondern hören Sie dem Referenten zu. Lesen Sie hier nicht weiter, sondern hören Sie dem Referenten zu. Lesen Sie hier nicht weiter, sondern hören Sie dem Referenten zu.

Warum wir wirklich hier sind

Klarheit über typische Begriffe schaffen

Wer betroffen und wer verantwortlich ist

Für jeden nachvollziehbare Beispiele sehen

Einfache Hilfsmittel mitnehmen, ohne Experte zu sein

# Risiko? Datensicherheit?

Die Definition von Risiko ist einfach.

„möglicher negativer Ausgang bei einer Unternehmung, mit dem Nachteile, Verlust, Schäden verbunden sind“ (Quelle: Duden)

Die Definition von Datensicherheit dagegen ist mehrdeutig belastet.

# Informationssicherheit

## Schutzziele zum Erhalt der Informationssicherheit

Vertraulichkeit (confidentiality)

Integrität (integrity)

Authentizität (authenticity)

Verfügbarkeit (availability)

Zurechenbarkeit (accountability)

## Gesetzliche Anforderungen

Datenschutz (data protection)

Basierend auf gesetzlichen Bestimmungen wie BStDG, Strafrecht, Sozialgesetzbuch, (später EU-Datenschutzgrundverordnung) etc.

# Wer ist betroffen?

## Privatsphäre

Jeder, der Informationen besitzt, die privat sind.

## Reaktion

Jeder, der aufgrund einer Nachricht, etwas tut.

## Gesetze

Jeder, der gesetzlichen Regularien unterworfen ist.

# Raum und Zeit der Daten

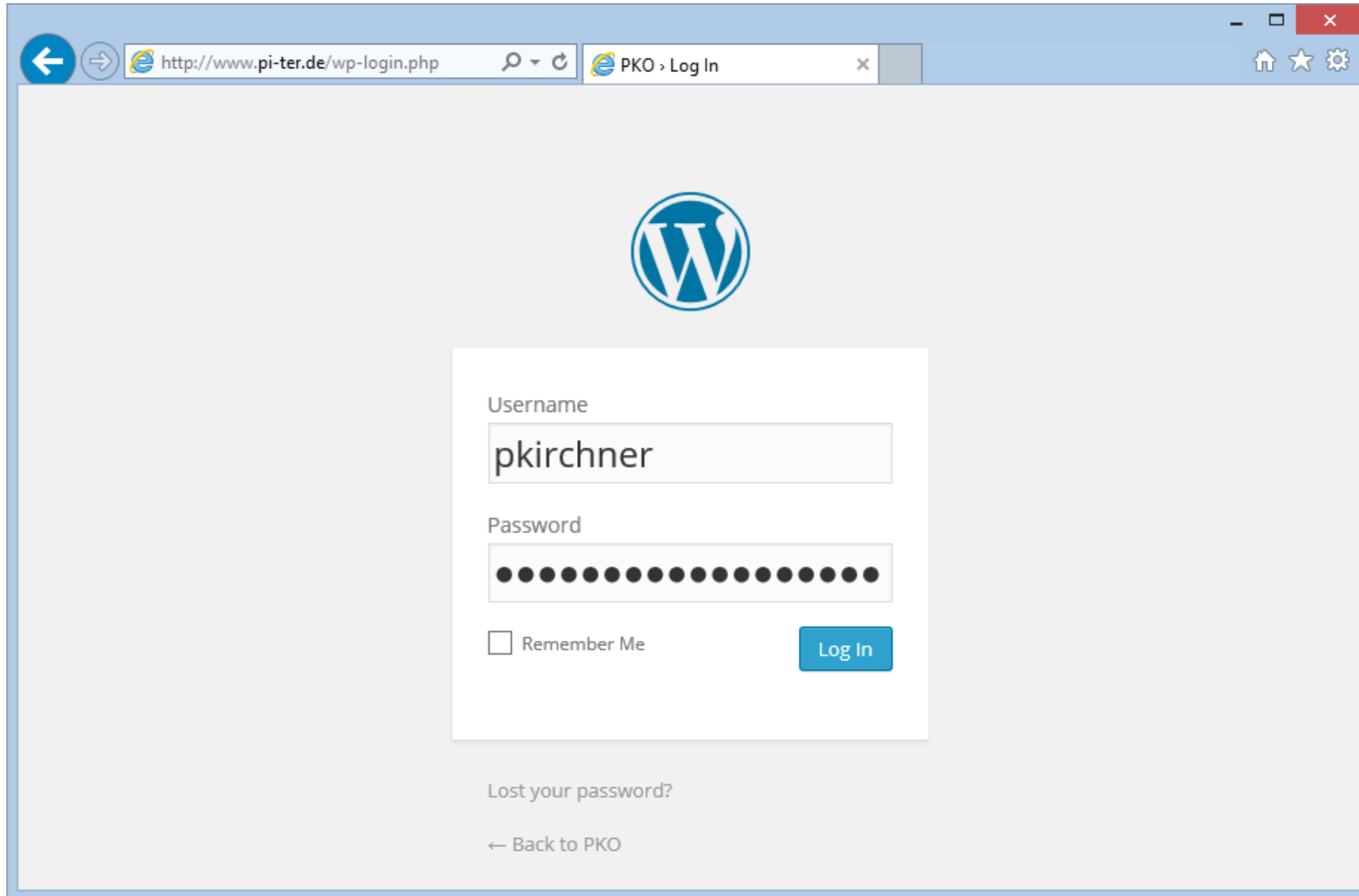
## Unterscheidung der Zustände der Daten

Data at Rest

Data in Motion/Transit

Data in Use

# Beispiel: Blog – Log In



The image shows a browser window with the URL `http://www.pi-ter.de/wp-login.php`. The page features the WordPress logo at the top center. Below the logo is a login form with the following elements:

- Username:** A text input field containing the text "pkirchner".
- Password:** A password input field represented by a series of black dots.
- Remember Me:** A checkbox labeled "Remember Me" which is currently unchecked.
- Log In:** A blue button labeled "Log In".

Below the login form, there is a link for "Lost your password?" and a link for "← Back to PKO".



# Beispiel: Blog – HTTP POST

```
21 <form name="loginform" id="loginform" action="http://www.pi-ter.de/wp-login.php" method="post">
22   <p>
23     <label for="user_login">Username<br />
24     <input type="text" name="log" id="user_login" class="input" value="" size="20" /></label>
25   </p>
26   <p>
27     <label for="user_pass">Password<br />
28     <input type="password" name="pwd" id="user_pass" class="input" value="" size="20" /></label>
29   </p>
30   <p class="forgetmenot"><label for="rememberme"><input name="rememberme" type="checkbox" id="rememberme" value="forever" />
31   <p class="submit">
32     <input type="submit" name="wp-submit" id="wp-submit" class="button button-primary button-large" value="Log In" />
33     <input type="hidden" name="redirect_to" value="http://www.pi-ter.de/wp-admin/" />
34     <input type="hidden" name="testcookie" value="1" />
35   </p>
36
```

# Beispiel: Blog – HTTP-Analyse mit Fiddler

POST http://www.pi-ter.de/wp-login.php HTTP/1.1

Accept: text/html, application/xhtml+xml, \*/\*

Referer: http://www.pi-ter.de/wp-login.php

Accept-Language: de-DE,de;q=0.8,en-GB;q=0.5,en;q=0.3

User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; Touch; rv:11.0) like Gecko

Content-Type: application/x-www-form-urlencoded

Accept-Encoding: gzip, deflate

Connect

Content

DNT: 1

Host: ww

Pragma:

Cookie: wp-settings-time-1=1409142076;

ARRAffinity=03b8571f470f874e6e24f0e5daa4ed9d929cd3b0f311fe4e212e90f8ba1e00a1;

wordpress\_test\_cookie=WP+Cookie+check

log=pkirchner&pwd=G4.Li9-DxVbq2%21xsTr&wp-submit=Log+In&redirect\_to=http%3A%2F%2Fwww.pi-ter.de%2Fwp-admin%2F&testcookie=1

#	Result	Protocol	Host	URL	Body	Caching	Content-Type	Process
1	200	HTTP	www.pi-ter.de	/wp-login.php	1.329	no-cache, must...	text/html; charset=UTF-8	iexplore:13752
8	302	HTTP	www.pi-ter.de	/wp-login.php	153	no-cache, must...	text/html; charset=UTF-8	iexplore:13752
9	200	HTTP	www.pi-ter.de	/wp-admin/	14.552	no-cache, must...	text/html; charset=UTF-8	iexplore:13752

# Beispiel: Blog – Netzwerkanalyse

The screenshot shows a Wireshark capture of network traffic. The main pane displays a list of packets, with packet 87 selected. The packet list shows:

No.	Time	Source	Destination	Protocol	Length	Info
83	10.251536000	10.141	10.141	TLSv1	144	Application Data, Application Data
84	10.288267000	141	10.	TCP	60	443-23895 [ACK] Seq=1 Ack=91 Win=2670 Len=0
85	10.698892000	10.	94.	ISAKMP	426	Unknown 243
86	10.699201000	10.	94.	ISAKMP	454	Identity Protection (Main Mode)
87	10.973846000	10.	65.	HTTP	776	POST /wp-login.php HTTP/1.1 (application/x-www-form-urlencoded)
88	11.054080000	65.	10.	TCP	60	80-15723 [ACK] Seq=6152 Ack=1952 win=514 Len=0
89	11.101052000	65.	10.	HTTP	1088	HTTP/1.1 302 Moved Temporarily (text/html)
90	11.101299000	10.	65.	TCP	54	15723-80 [ACK] Seq=1952 Ack=7186 win=1024 Len=0
91	11.106916000	10.	65.	HTTP	906	GET /wp-admin/ HTTP/1.1
92	11.254244000	65.	10.	TCP	60	80-15723 [ACK] Seq=7186 Ack=2804 win=511 Len=0
93	11.398187000	65.	10.	TCP	1440	[TCP segment of a reassembled PDU]
94	11.398360000	10.	65.	TCP	54	15723-80 [ACK] Seq=2804 Ack=8572 win=1024 Len=0
95	11.398814000	65.	10.	TCP	1440	[TCP segment of a reassembled PDU]
96	11.398816000	65.	10.	TCP	1440	[TCP segment of a reassembled PDU]
97	11.398818000	65.	10.	TCP	1440	[TCP segment of a reassembled PDU]
98	11.398828000	65.	10.	TCP	1440	[TCP segment of a reassembled PDU]

The packet details pane for packet 87 shows the following structure:

- Accept-Encoding: gzip, deflate\r\n
- Host: www.pi-ter.de\r\n
- Content-Length: 121\r\n
- DNT: 1\r\n
- Connection: Keep-Alive\r\n
- Cache-Control: no-cache\r\n
- Cookie: wp-settings-time=1409142221; ARRAffinity=03b8571f470f874e6e24f0e5daa4ed9d929cd3b0f311fe4e212e90f8ba1e00a1; wordpress\_test\_cookie=WP+Cookie\r\n
- [Full request URI: <http://www.pi-ter.de/wp-login.php>]
- [HTTP request 4/5]
- [Prev request in frame: 55]
- [Response in frame: 89]
- [Next request in frame: 91]
- HTML Form URL Encoded: application/x-www-form-urlencoded
  - Form item: "log" = "pkirchner"
    - Key: log
    - Value: pkirchner
  - Form item: "pwd" = "G4.Li9-Dxvbq2!xsTr"
    - Key: pwd
    - Value: G4.Li9-Dxvbq2!xsTr

The packet bytes pane shows the raw data of the request, including the cookie and form data.

Form item (urlencoded-form), 25 bytes | Packets: 141 - Displayed: 141 (100,0%) - Dropped: 0 (0,0%) | Profile: Default

# Beispiel: Program Data von Apps ab Windows 8

The screenshot displays the Windows Explorer interface. The address bar shows the path: `Dieser PC > OSDisk (C:) > Programme > WindowsApps > WindowsApps\Microsoft.Windows.Common-Platform_1.0.9.94_x64_8ptj331gd3tyt`. The left pane shows the navigation tree with 'WindowsApps' expanded. The right pane shows a list of files and folders for the selected app. The 'App' folder is selected, and its contents are shown in the right pane.

Name	Änderungsdatum	Typ	Größe
AppxMetadata	10.07.2014 16:04	Dateiordner	
Assets	10.07.2014 16:04	Dateiordner	
Camera	10.07.2014 16:04	Dateiordner	
Common	10.07.2014 16:04	Dateiordner	
EmojiStickerModule	10.07.2014 16:04	Dateiordner	
Resources	10.07.2014 16:04	Dateiordner	
SampleData	10.07.2014 16:04	Dateiordner	
TalkBizModule	10.07.2014 16:04	Dateiordner	
UI	10.07.2014 16:04	Dateiordner	
App	17.06.2014 13:09	Windows-Markup...	4 KB
AppxBlockMap	10.07.2014 16:04	XML Document	134 KB
AppxManifest	10.07.2014 16:04	XML Document	5 KB
AppxSignature.p7x	10.07.2014 16:04	P7X-Datei	11 KB
...	10.07.2014 16:04	Anwendungserwe...	52 KB
...	10.07.2014 16:04	Anwendungserwe...	96 KB
...	10.07.2014 16:04	Anwendungserwe...	35 KB
...	10.07.2014 16:04	Anwendungserwe...	49 KB
...	10.07.2014 16:04	Anwendungserwe...	62 KB
...	10.07.2014 16:04	Anwendungserwe...	17 KB
...	10.07.2014 16:04	Anwendung	744 KB
...	10.07.2014 16:04	Anwendungserwe...	25 KB
...	10.07.2014 16:04	Anwendungserwe...	65 KB
...	10.07.2014 16:04	WINMD-Datei	52 KB
...	17.06.2014 13:09	PRI-Datei	233 KB
...	10.07.2014 16:04	Anwendungserwe...	1.171 KB
...	10.07.2014 16:04	WINMD-Datei	7 KB



# Beispiel: App Data ab Windows 8

```
000013b0 49 73 41 75 74 6F 4C 6F 67 69 6E 00 00 00 00 00 IsAutoLogin.....
000013c0 F0 FF FF FF 01 F3 A6 EC D0 5F 9C CF 01 00 00 00 .....vk.....
000013d0 E0 FF FF FF 76 6B 06 00 34 00 00 00 F0 03 00 00 .....vk.4.....
000013e0 .....UserId..
000013f0 .....m.a.i.l.@.
00001400
00001410
00001420 D2 EC 4A 21 2E A0 CF 01 E8 FF FF FF 18 01 00 00 ..J!.....
00001430 68 02 00 00 98 03 00 00 D0 03 00 00 40 04 00 00 h.....@...
00001440 D8 FF FF FF 76 6B 0C 00 2A 00 00 00 68 04 00 00 .....vk.*...h...
00001450 .....UserPass
00001460 word.....h.Z.
00001470
00001480 z.9.J.7.A.=.....
00001490 4B 21 2E A0 CF 01 00 00 98 FF FF FF 6E 6B 20 00 K!.....nk .
000014a0 71 3F CE 67 62 A0 CF 01 00 00 00 00 08 02 00 00 q?.gb.....
000014b0 00 00 00 00 00 00 00 00 FF FF FF FF FF FF FF FF .....
000014c0 0A 00 00 00 18 0A 00 00 68 01 00 00 FF FF FF FF .....h.....
000014d0 00 00 00 00 00 00 00 00 4C 00 00 00 24 00 00 00 .....L...$.
000014e0 .....mail@
000014f0 .....de...
00001500 D0 FF FF FF 76 6B 12 00 10 00 00 00 30 05 00 00 .....vk.....0...
00001510 06 E1 F5 05 01 00 00 00 54 41 42 45 4C 5F 56 45 .....TABEL_VE
00001520 52 53 49 4F 4E 5F 43 68 61 74 00 00 00 00 00 00 RSION_Chat.....
00001530 E8 FF FF FF 01 00 00 00 00 00 00 00 06 52 82 21 .....R.!
00001540 2E A0 CF 01 00 00 00 00 D0 FF FF FF 76 6B 15 00 .....vk..
00001550 10 00 00 00 78 05 00 00 06 E1 F5 05 01 00 00 00 .....x.....
00001560 54 41 42 45 4C 5F 56 45 52 53 49 4F 4E 5F 53 74 TABEL_VERSION_St
00001570
```

```
00001580 .....vp.....
00001590 F0 FF FF FF 01 00 00 00 5D 6E 37 A1 1D 8A CF 01 .....]n7.....
000015a0 C8 FF FF FF 76 6B 18 00 09 00 00 00 08 01 00 00 .....vk.....
000015b0 0B E1 F5 05 01 00 00 00 4E 6F 74 69 66 69 63 61 .....Notifica
000015c0 74 69 6F 6E 44 69 73 61 62 6C 65 64 57 69 74 68 tionDisabledWith
000015d0 53 75 62 00 00 00 00 00 68 00 00 00 76 6B 24 00 Sub.....h...vk$.
000015e0 0C 00 00 00 18 06 00 00 04 E1 F5 05 01 00 00 00 .....
000015f0 55 52 5F 63 35 65 38 34 32 38 36 64 32 63 35 35 UR_c5e84286d2c55
00001600 36 31 34 30 66 37 62 66 38 66 65 37 35 34 61 66 6140f7bf8fe754af
00001610 33 66 66 35 00 00 00 00 28 00 00 00 01 00 00 00 3ff5....(.....
00001620 F8 19 83 43 5D A0 CF 01 18 00 00 00 07 00 00 00 ...C].....
00001630 58 73 FB 11 25 A0 CF 01 08 00 00 00 40 06 00 00 Xs.%.....@...
00001640 C0 FF FF FF 76 6B 25 00 0C 00 00 00 90 05 00 00 .....vk%.....
00001650 04 E1 F5 05 01 00 00 00 4B 45 59 5F 4C 41 53 54 .....KEY_LAST
00001660
00001670
00001680 C0 FF FF FF 76 6B 26 00 24 00 00 00 C0 06 00 00 .....vk&.$.....
00001690 0C E1 F5 05 01 00 00 00 4C 52 4D 50 5F 75 62 34 .....LRMP_ub4
000016a0 36 31 62 38 61 31 31 30 31 36 65 36 61 32 34 34 61b8a11016e6a244
000016b0 39 63 38 35 65 64 31 63 37 62 31 35 39 37 00 00 9c85ed1c7b1597..
000016c0 D8 FF FF FF 31 00 34 00 30 00 33 00 32 00 32 00 ....1.4.0.3.2.2.
000016d0 39 00 36 00 36 00 33 00 39 00 33 00 35 00 00 00 9.6.6.3.9.3.5...
000016e0 B2 D8 C4 83 5E 9C CF 01 08 00 00 00 80 06 00 00 ....^.....
000016f0 C0 FF FF FF 76 6B 26 00 24 00 00 00 30 07 00 00 .....vk&.$...0...
00001700 0C E1 F5 05 01 00 00 00 4C 52 4D 50 5F 63 66 38 .....LRMP_cf8
00001710 32 35 38 33 36 64 32 34 35 63 30 37 61 30 32 31 25836d245c07a021
00001720 65 65 30 30 32 36 37 65 33 66 63 33 64 32 00 00 ee00267e3fc3d2..
00001730 D8 FF FF FF 31 00 34 00 32 00 30 00 38 00 34 00 ....1.4.2.0.8.4.
00001740 37 00 31 00 38 00 35 00 32 00 38 00 36 00 00 00 7.1.8.5.2.8.6...
00001750 B3 5A 71 43 5D A0 CF 01 C0 FF FF FF 76 6B 26 00 7aC1 .....vk&
```

# Beispiel: Security by Obscurity

```
CommonUtility.cs  Logger.cs  Login .cs  Session .cs  Auth .cs  Password .cs X
// Decompiled with JetBrains decompiler
// Type: [REDACTED]
// Assembly: [REDACTED], Version=1.0.0.0, Culture=neutral, PublicKeyToken=null
// MVID: [REDACTED]
// Assembly location: C:\Program Files\WindowsApps\[REDACTED].dll

namespace [REDACTED]
{
    public class Password [REDACTED]
    {
        private string _even;
        private string _odd;

        public void SetPassword(string password)
        {
            this._even = string.Empty;
            this._odd = string.Empty;
            for (int index = 0; index < password.Length; ++index)
            {
                if (index % 2 == 0)
                {
                    [REDACTED] = this;
                    string str = [REDACTED]._even + (object) password[index];
                    [REDACTED]._even = str;
                }
            }
        }
    }
}
```

# Probleme und Herausforderungen

Sicherheit ist kompliziert und braucht Erfahrung

Sicherheit ist schwer zu testen

Sicherheit der Superlativen

gerade im Marketing

Sicherheit benötigt Vertrauen

Softwarehersteller wählen und vertrauen auf Technologien

Kunden beziehen und vertrauen auf Software

*Etwas darf nicht nur sicher sein, sondern  
muss auch sicher wirken. (Bruce Schneier)*

# Auswahl der Technologie

## Zahlreiche Bibliotheken, Frameworks und APIs

System.Security.Cryptography

Windows.Security.Cryptography

Microsoft CryptoAPI

Cryptography API: Next Generation (CNG)

## Kriterien für die Auswahl

Verfügbarkeit für Plattformen und Entwicklungssprache

Funktionsumfang

Vertrauen



# Demo: Verschlüsselung mit Windows.Security.Cryptography

```
public static IBuffer Encrypt(  
    CryptographicKey key,  
    IBuffer data,  
    IBuffer iv  
)
```

```
public static IBuffer Decrypt(  
    CryptographicKey key,  
    IBuffer data,  
    IBuffer iv  
)
```

# CryptographicEngine

Method	Description
Decrypt	Decrypts content that was previously encrypted by using a symmetric or asymmetric algorithm.
DecryptAndAuthenticate	Decrypts and authenticates data.
DecryptAsync	Decrypts the encrypted input data using the supplied key.
DeriveKeyMaterial	Derives a key from another key by using a key derivation function.
Encrypt	Encrypts data by using a symmetric or asymmetric algorithm.
EncryptAndAuthenticate	Performs authenticated encryption.
Sign	Signs digital content.
SignAsync	Computes a hash for the supplied input data, and then signs the computed hash using the specified key.
SignHashedData	Signs the hashed input data using the specified key.
SignHashedDataAsync	Signs the hashed input data using the specified key.
VerifySignature	Verifies a message signature.
VerifySignatureWithHashInput	Verifies the signature of the specified input data against a known signature.

# Beispiel: Symmetrische Verschlüsselung mit Windows.Security.Cryptography

```
// Create a buffer that contains the encoded message to be encrypted.
IBuffer buffMsg = CryptographicBuffer
    .ConvertStringToBinary("Vertrauliche Nachricht",
        BinaryStringEncoding.Utf8);

// Open a symmetric algorithm provider for the specified algorithm.
SymmetricKeyAlgorithmProvider skaProvider =
    SymmetricKeyAlgorithmProvider.OpenAlgorithm
        (SymmetricAlgorithmNames.AesCbcPkcs7);

// Create a symmetric key.
IBuffer keyMaterial = CryptographicBuffer
    .GenerateRandom(/* key length */256);
CryptographicKey key = skaProvider.CreateSymmetricKey(keyMaterial);
```

# Beispiel: Symmetrische Verschlüsselung mit Windows.Security.Cryptography

```
// CBC algorithms require an initialization vector.  
// Here, a random number is used for the vector.  
IBuffer iv = CryptographicBuffer.GenerateRandom(skaProvider.BlockLength);  
  
// Encrypt the data and return.  
IBuffer buffEncrypt = CryptographicEngine.Encrypt(key, buffMsg, iv);  
  
return buffEncrypt;
```

# Hilfsklasse CryptographicBuffer

Method	Description
Compare	Compares two IBuffer objects.
ConvertBinaryToString	Converts a buffer to an encoded string.
ConvertStringToBinary	Converts a string to an encoded buffer.
CopyToByteArray	Copies a buffer to an array of bytes.
CreateFromByteArray	Creates a buffer from an input byte array.
DecodeFromBase64String	Decodes a string that has been base64 encoded.
DecodeFromHexString	Decodes a string that has been hexadecimal encoded.
EncodeToBase64String	Encodes a buffer to a base64 string.
EncodeToHexString	Encodes a buffer to a hexadecimal string.
GenerateRandom	Creates a buffer that contains random data.
GenerateRandomNumber	Creates a random number.

# Transportsicherung

Data in Motion/Transit

Vertraulichkeit während der Kommunikation

Einfachste Sicherungsmaßnahme: SSL / TLS

Aber: SSL & TLS ist in nicht-vertrauenswürdigen Netzwerken nicht sicher

Siehe: DEFCON 17: More Tricks For Defeating SSL (<https://www.youtube.com/watch?v=ibF36Yyeehw>)

# SSL-Zertifikate prüfen am Beispiel Windows Runtime

## Klasse `HttpTransportInformation`

Namensraum `Windows.Web.Http`

## Methode `Certificate.BuildChainAsync`

Namensraum `Windows.Security.Cryptography.Certificates`

## Ergebnis `ChainValidationResult`

# Enumeration ChainValidationResult

14 mögliche Prüfungsergebnisse...

Member	Value	Description
Success   success	0	The certificate chain was verified.
Untrusted   untrusted	1	A certificate in the chain is not trusted.
Revoked   revoked	2	A certificate in the chain has been revoked.
Expired   expired	3	A certificate in the chain has expired.
IncompleteChain   incompleteChain	4	The certificate chain is missing one or more certificates.
InvalidSignature   invalidSignature	5	The signature of a certificate in the chain cannot be verified.
WrongUsage   wrongUsage	6	A certificate in the chain is being used for a purpose other than one specified by its CA.
InvalidName   invalidName	7	A certificate in the chain has a name that is not valid. The name is either not included in the permitted list or is explicitly excluded.
InvalidCertificateAuthorityPolicy   invalidCertificateAuthorityPolicy	8	A certificate in the chain has a policy that is not valid.



# Defence in Depth

## Misstrauen gegenüber scheinbar vertrauenswürdigen Schichten und Komponenten

Prüfung von Daten

Prüfung der Kommunikationspartner

Sicherung „interner“ Kommunikation

Einschränkung der Kommunikationsrichtung

## Assume Breach

Grundlegender Wandel von Design und Architekturen

# Security Development Lifecycle (SDL)

Definierte und relevante Sicherheitsmaßnahmen in jedem Entwicklungsschritt

## What is the Security Development Lifecycle ?



The Security Development Lifecycle (SDL) is a software development process that helps developers build more secure software and address security compliance requirements while reducing development cost.

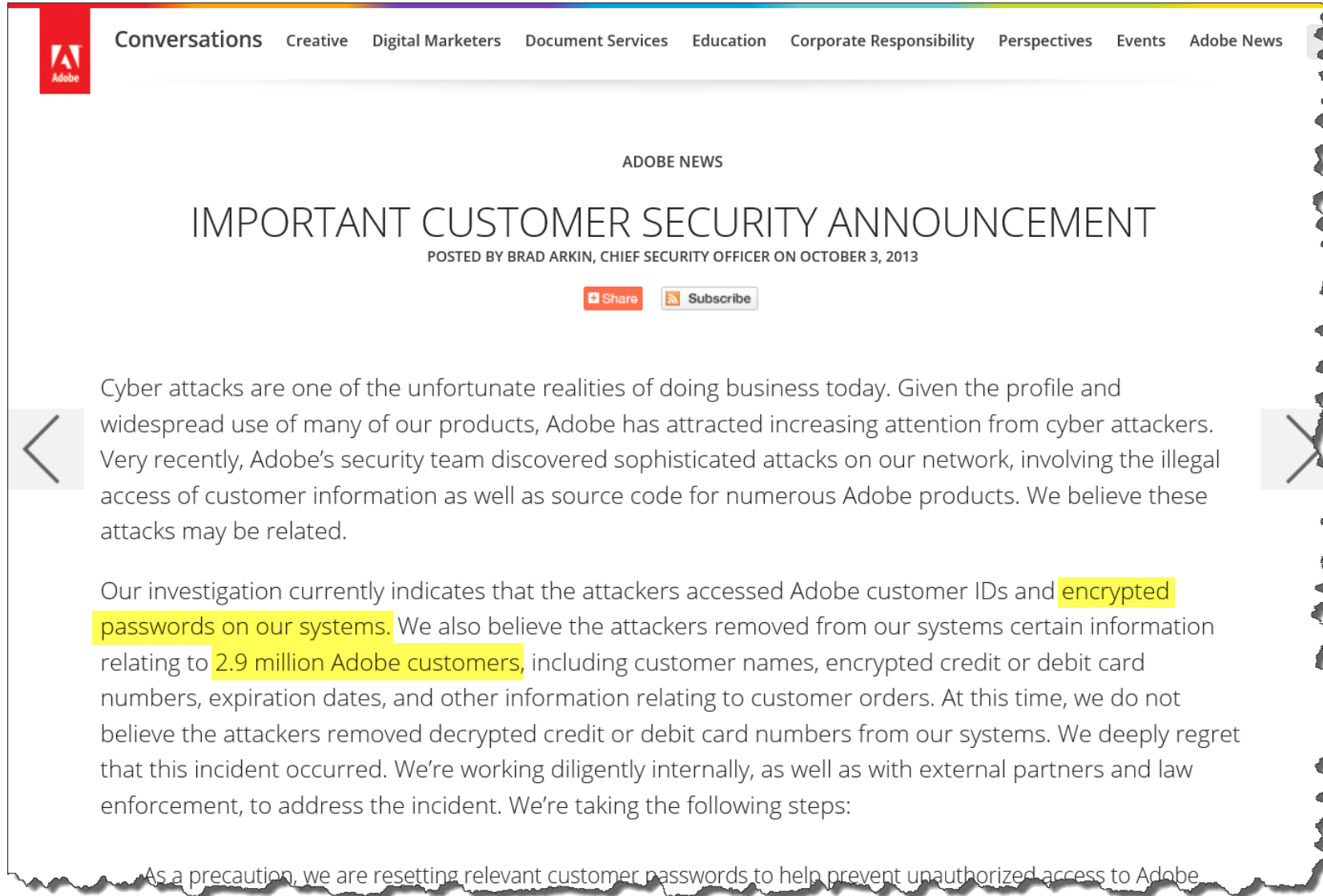


# Das schwächste Glied



Quelle: <https://www.youtube.com/watch?v=a6iW-8xPw3k>

# Beispiel: Adobe

The image shows a screenshot of an Adobe blog post. At the top left is the Adobe logo. A navigation bar contains links for Conversations, Creative, Digital Marketers, Document Services, Education, Corporate Responsibility, Perspectives, Events, and Adobe News. The main heading is 'ADOBE NEWS' followed by 'IMPORTANT CUSTOMER SECURITY ANNOUNCEMENT'. Below the heading is the text 'POSTED BY BRAD ARKIN, CHIEF SECURITY OFFICER ON OCTOBER 3, 2013'. There are 'Share' and 'Subscribe' buttons. The main text describes a cyber attack on Adobe's systems, mentioning that customer IDs and encrypted passwords were accessed, and that 2.9 million Adobe customers' information was affected. The text is highlighted in yellow. At the bottom, it says 'As a precaution, we are resetting relevant customer passwords to help prevent unauthorized access to Adobe'.

Quelle: <http://blogs.adobe.com/conversations/2013/10/important-customer-security-announcement.html>

# Beispiel: Adobe

Was ging schief?

Passwort Hints im Klartext

ECB statt CBC

Passworte verschlüsselt  
statt Hashes

HACKERS RECENTLY LEAKED 153 MILLION ADOBE USER EMAILS, ENCRYPTED PASSWORDS, AND PASSWORD HINTS. ADOBE ENCRYPTED THE PASSWORDS IMPROPERLY, MISUSING BLOCK-MODE 3DES. THE RESULT IS SOMETHING WONDERFUL:

USER	PASSWORD	HINT	
4e18acc1ab27a2d6		WEATHER VANE SWORD	<input type="text"/>
4e18acc1ab27a2d6			<input type="text"/>
4e18acc1ab27a2d6	a0a2876eb1ea1fca	NAME 1	<input type="text"/>
8bab66299e06eb6d		DUH	
8bab66299e06eb6d	a0a2876eb1ea1fca		<input type="text"/>
8bab66299e06eb6d	85e9da81a8a78adc	57	
4e18acc1ab27a2d6		FAVORITE OF 12 APOSTLES	
1ab29ae86dab6e5ca	7a2d6a0a2876eb1e	WITH YOUR OWN HAND YOU HAVE DONE ALL THIS	
a1f9b2b6299e7a2b	e0dec1e6ab797397	SEXY EARLOBES	<input type="text"/>
a1f9b2b6299e7a2b	617ab0277727ad85	BEST TOS EPISODE	<input type="text"/>
39738b7adb0b8af7	617ab0277727ad85	SUGARLAND	<input type="text"/>
1ab29ae86dab6e5ca		NAME + JERSEY #	
877ab7889d3862b1		ALPHA	<input type="text"/>
877ab7889d3862b1			<input type="text"/>
877ab7889d3862b1			<input type="text"/>
877ab7889d3862b1			<input type="text"/>
877ab7889d3862b1		OBVIOUS	<input type="text"/>
877ab7889d3862b1		MICHAEL JACKSON	
38a7c9279codeb44	9dca1d79d4dec6d5		
38a7c9279codeb44	9dca1d79d4dec6d5	HE DID THE MASH, HE DID THE PURLOINED	<input type="text"/>
38a7c9279codeb44			<input type="text"/>
08ae5745a2b7af7a	9dca1d79d4dec6d5	FAV. LATER-3 POKEMON	

THE GREATEST CROSSWORD PUZZLE  
IN THE HISTORY OF THE WORLD

Quelle:  
<http://xkcd.com/1286/>



# Beispiele: Passworte

## WORST PASSWORDS OF 2013

rank	password	change from 2012
#01	123456	⬆️1
#02	password	⬇️1
#03	12345678	—
#04	qwerty	⬆️1
#05	abc123	⬇️1
#06	123456789	new
#07	111111	⬆️2
#08	1234567	⬆️5
#09	iloveyou	⬆️2
#10	adobe123	new



4.7% aller Nutzer verwenden das Passwort PASSWORD

8.5% nutzen PASSWORD oder 123456

9.8% nutzen PASSWORD oder 123456 oder 12345678

# Mehrheit oder Minderheit?

14% haben ein Passwort der Top 10

40% haben ein Passwort der Top 100

79% haben ein Passwort der Top 500

91% haben ein Passwort der Top 1000

# Wie können wir helfen?

## Aufklärung

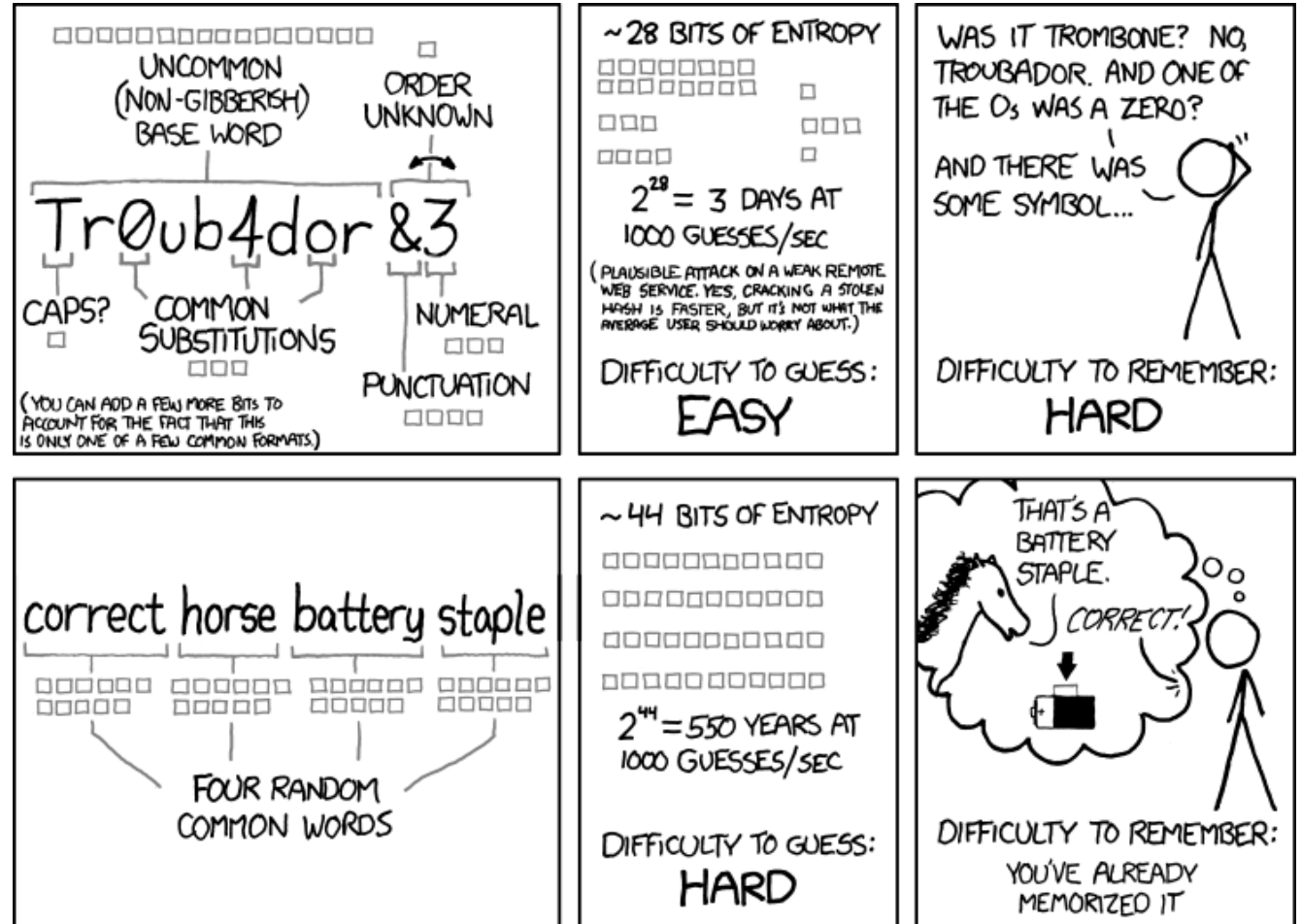
Bewusstsein für Sicherheit schaffen

## Sinnvolle Passwort-Beschränkungen

Länge & Zeichensatz

Komplexität

Projekte/APIs wie [Telepathwords](#)



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Quelle: <http://xkcd.com/936/>



# Weitere Informationen

□ Peter.Kirchner  
@Microsoft.com

□ [blogs.msdn.com/  
pkirchner](https://blogs.msdn.com/pkirchner)

□ Twitter:  
@peterkirchner

Microsoft Azure  
30 Tage kostenfrei testen  
[bit.ly/AzureAnmeldung](https://bit.ly/AzureAnmeldung)

Startseite von  
Microsoft Azure  
[azure.microsoft.com](https://azure.microsoft.com)

Office 365 testen  
[www.office.com](https://www.office.com)

