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 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. 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 BSDG, 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

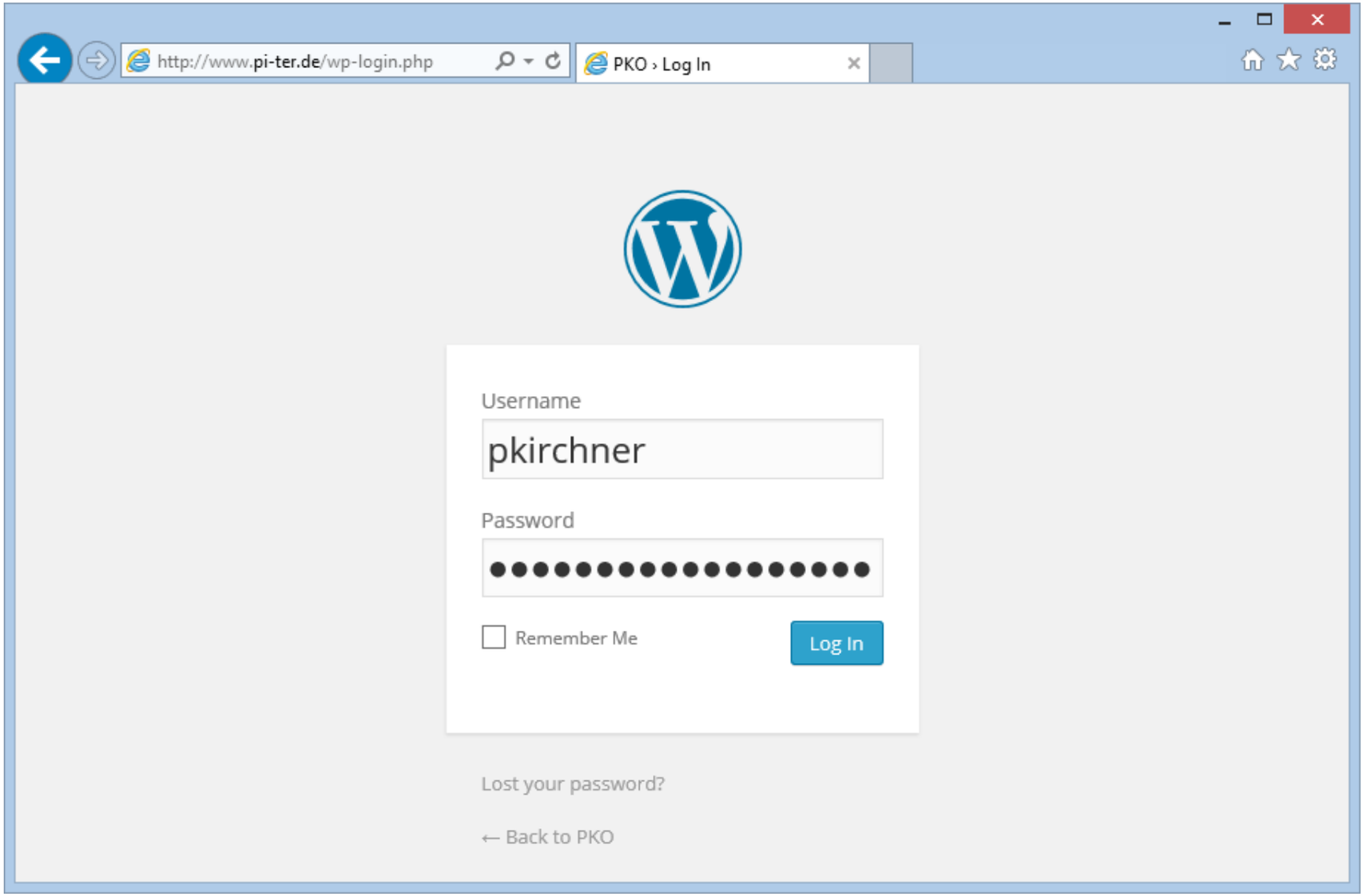
Jeder, der gesetzlichen Regularien unterworfen ist.

Raum und Zeit der Daten

Unterscheidung der Zustände der Daten

Data at Rest
Data in Motion/Transit
Data in Use

Beispiel: Blog – Log In



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
```

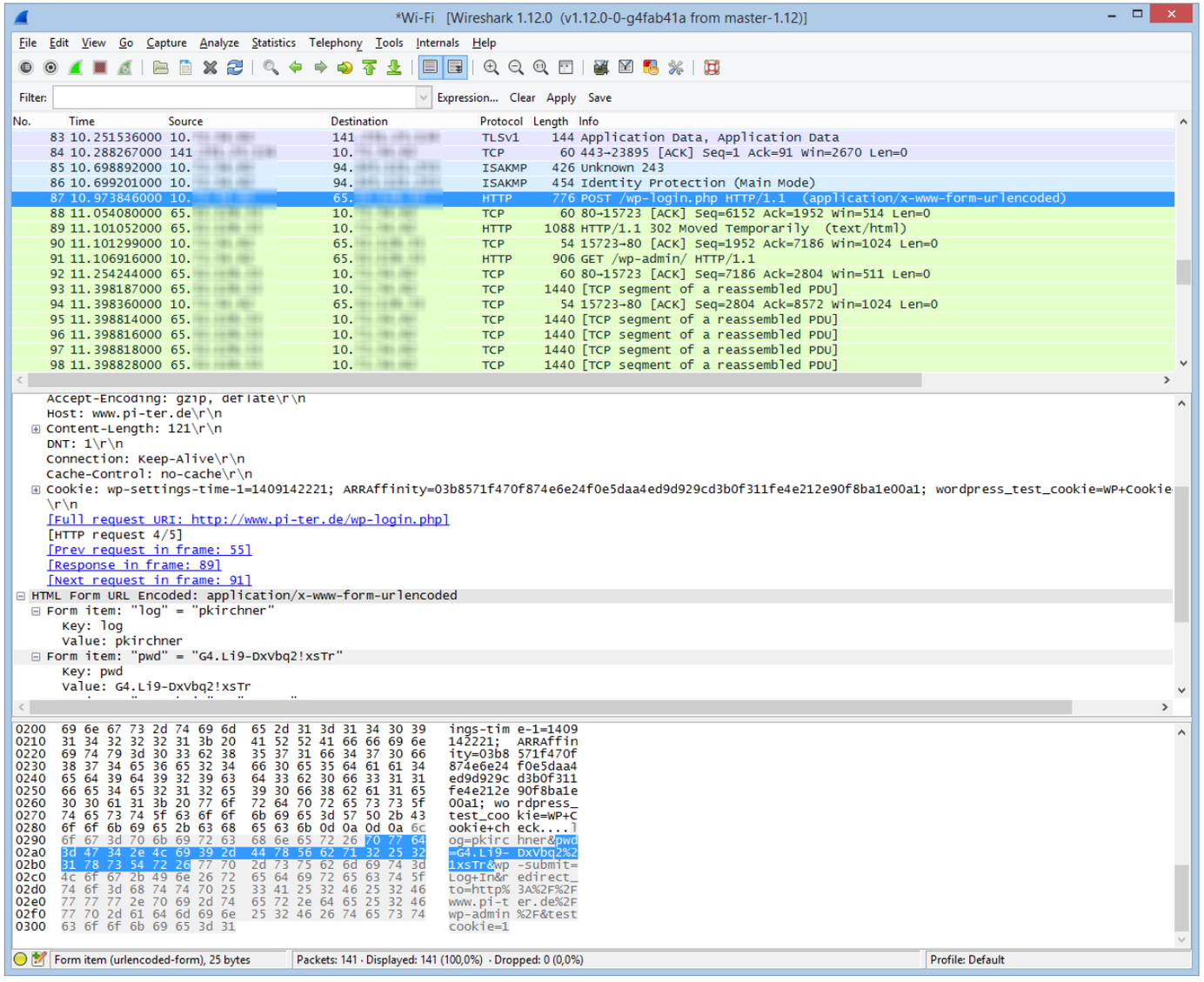
Beispiel: Blog – HTTP-Analyse mit Fiddler

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

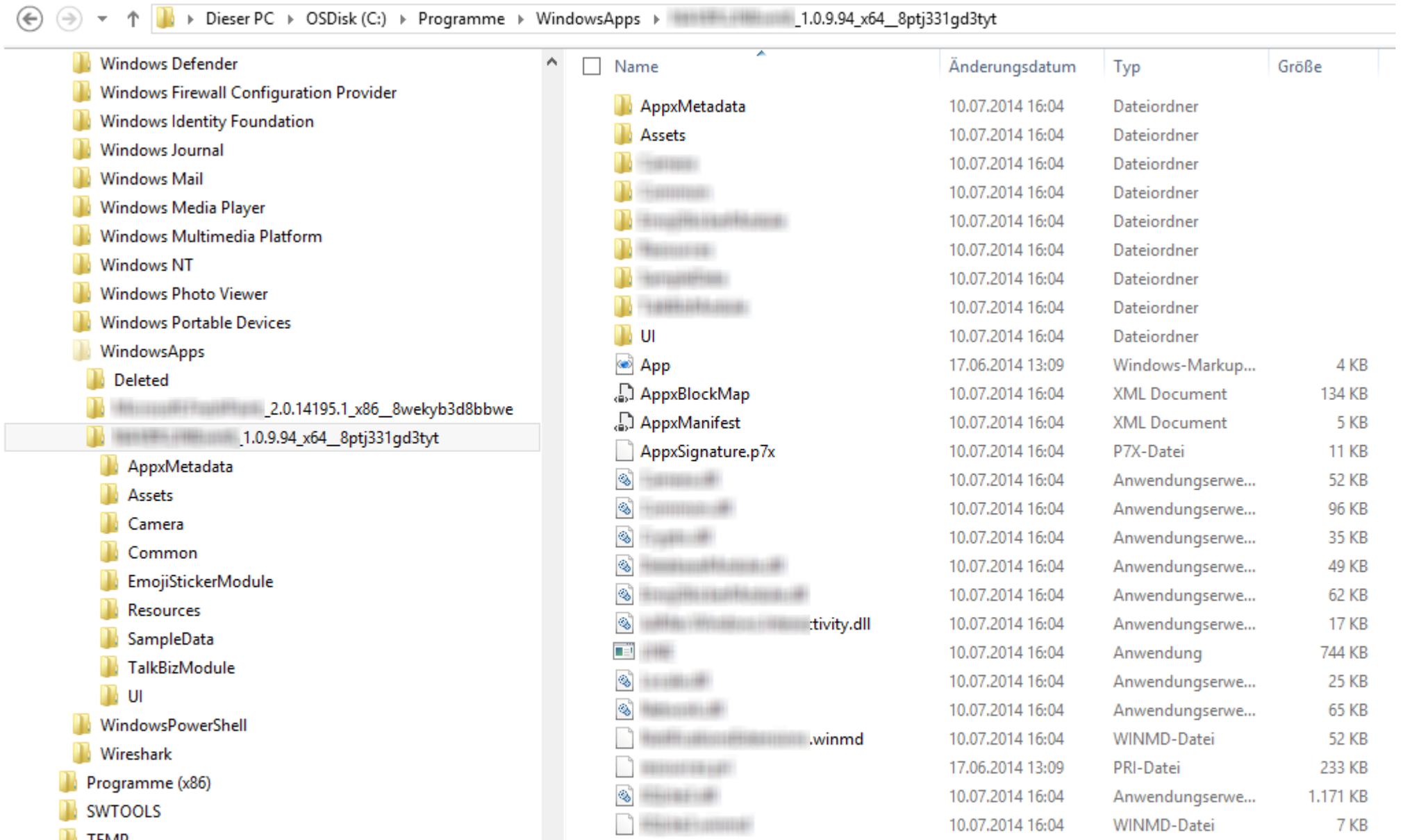
log=pkirchner&pwd=G4.Li9-DxVbq2%21xsTr&wp-submit=Log+In&redirect_to=http%3A%2F%2Fwww.pi-ter.de%2Fwp-admin%2F&testcookie=1

#	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

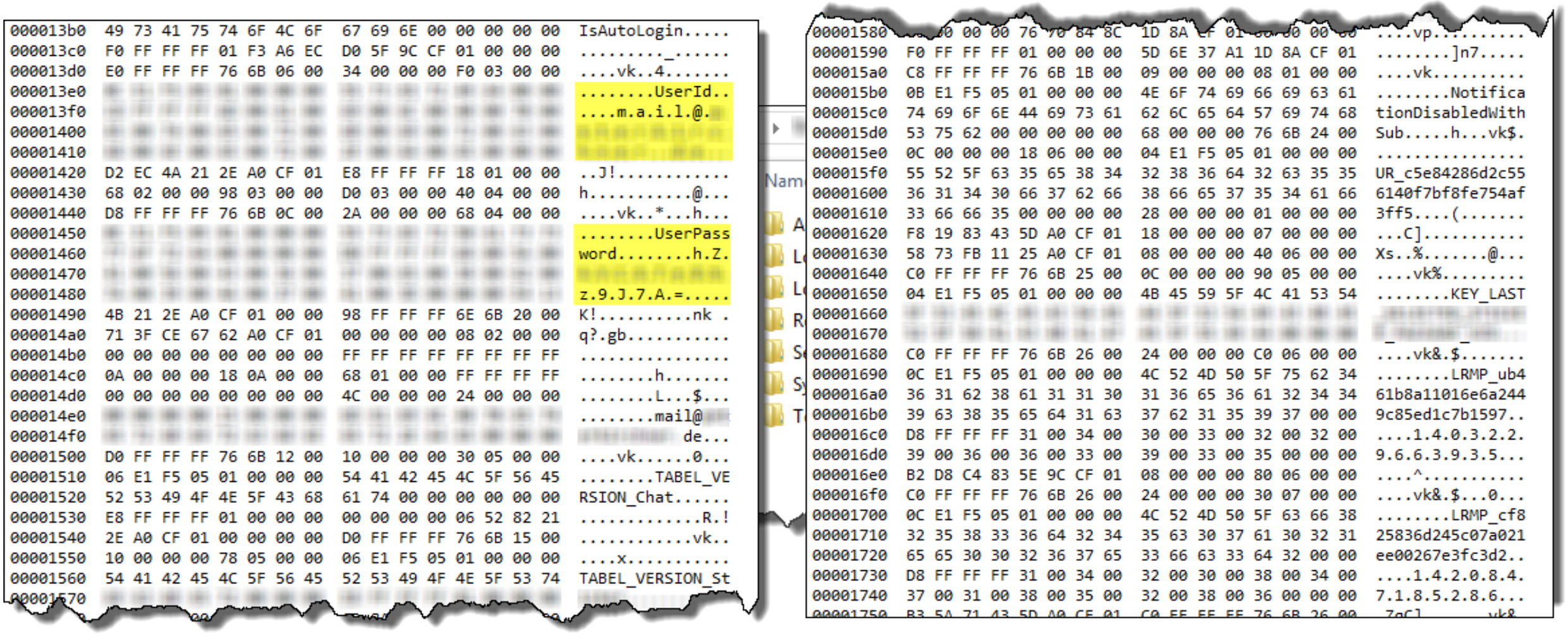
Beispiel: Blog – Netzwerkanalyse



Beispiel: Program Data von Apps ab Windows 8



Beispiel: App Data ab Windows 8



Beispiel: Security by Obscurity

CommonUtility.cs | Logger.cs | Login[illegible].cs | Session[illegible].cs | Auth[illegible].cs | Password[illegible].cs

```
// Decompiled with JetBrains decompiler
// Type: [illegible]
// Assembly: [illegible], Version=1.0.0.0, Culture=neutral, PublicKeyToken=null
// MVID: [illegible]
// Assembly location: C:\Program Files\WindowsApps\[illegible].dll

namespace [illegible]
{
  public class Password[illegible]
  {
    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)
        {
          [illegible] = this;
          string str = [illegible]._even + (object) password[index];
          [illegible]._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 Prüfungsresultate…

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

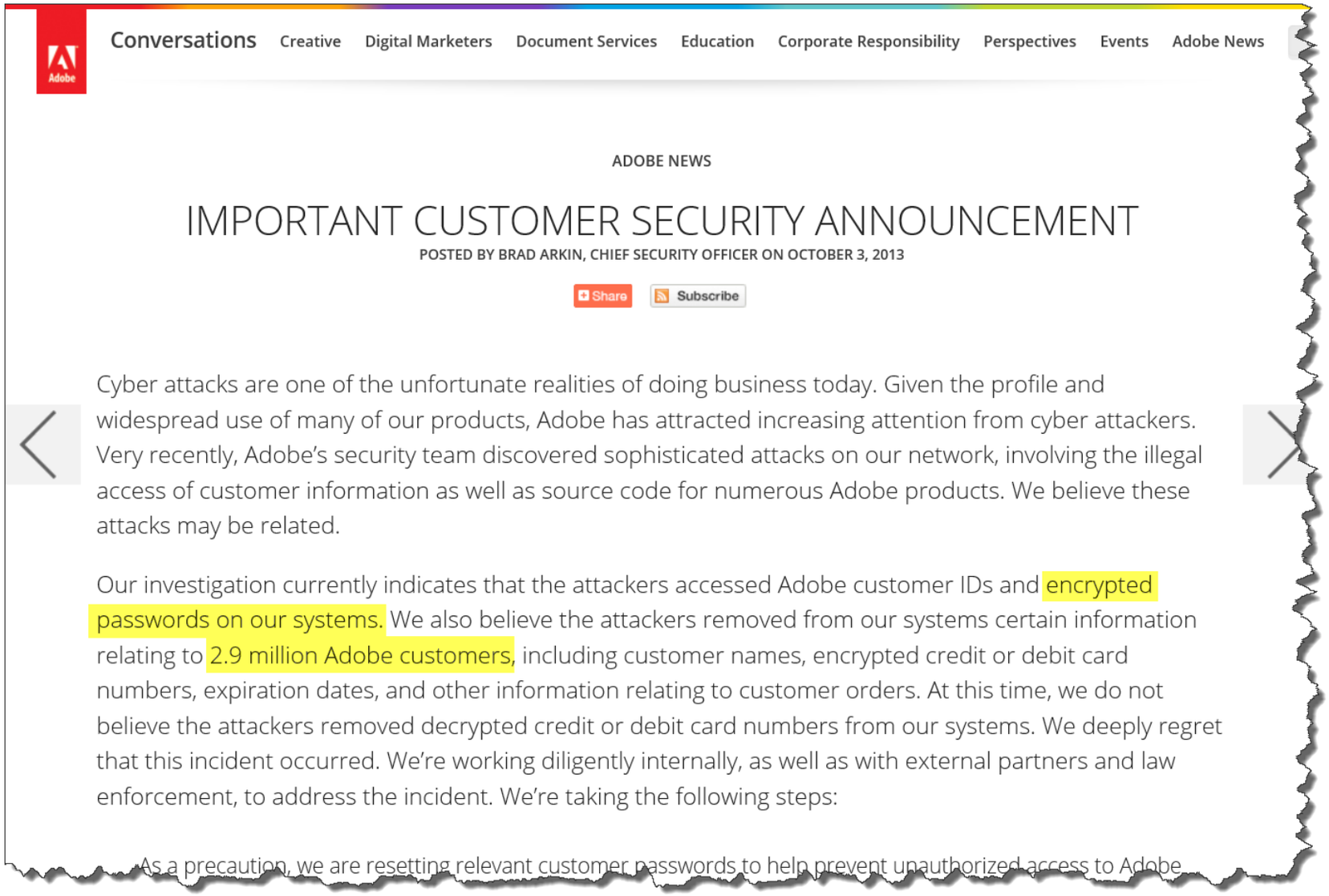
What is the Security Development Lifecycle ?

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



Conversations Creative Digital Marketers Document Services Education Corporate Responsibility Perspectives Events Adobe News

ADOBE NEWS

IMPORTANT CUSTOMER SECURITY ANNOUNCEMENT

POSTED BY BRAD ARKIN, CHIEF SECURITY OFFICER ON OCTOBER 3, 2013

Share Subscribe

Cyber attacks are one of the unfortunate realities of doing business today. Given the profile and widespread use of many of our products, Adobe has attracted increasing attention from cyber attackers. Very recently, Adobe's security team discovered sophisticated attacks on our network, involving the illegal access of customer information as well as source code for numerous Adobe products. We believe these attacks may be related.

Our investigation currently indicates that the attackers accessed Adobe customer IDs and encrypted passwords on our systems. We also believe the attackers removed from our systems certain information relating to 2.9 million Adobe customers, including customer names, encrypted credit or debit card numbers, expiration dates, and other information relating to customer orders. At this time, we do not believe the attackers removed decrypted credit or debit card numbers from our systems. We deeply regret that this incident occurred. We're working diligently internally, as well as with external partners and law enforcement, to address the incident. We're taking the following steps:

- 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

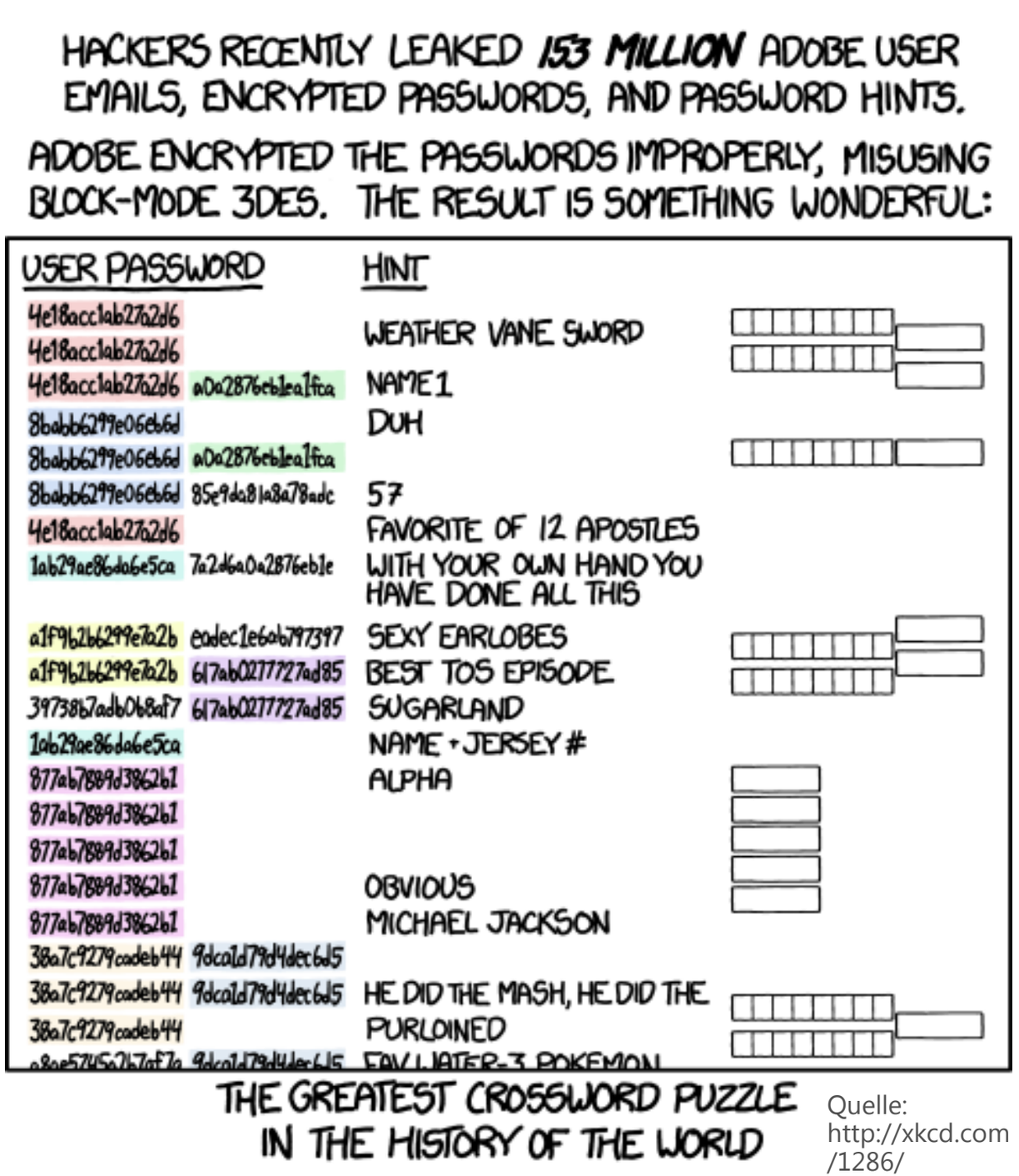
Beispiel: Adobe

Was ging schief?

Passwort Hints im Klartext

ECB statt CBC

Passworte verschlüsselt statt Hashes



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

Beispiele: Passworte

Quelle: http://splashdata.com/press/worstpasswords2013.htm

4.7% aller Nutzer verwenden das Passwort PASSWORD

8.5% nutzen PASSWORD oder 123456

9.8% nutzen PASSWORD oder 123456 oder 12345678

Quelle: Tim Messerschmidt / @SeraAndroiD Lead Developer Evangelist, EMEA Developer Week '14

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

Quelle: Tim Messerschmidt / @SeraAndroiD Lead Developer Evangelist, EMEA Developer Week ‘14

Wie können wir helfen?

Aufklärung

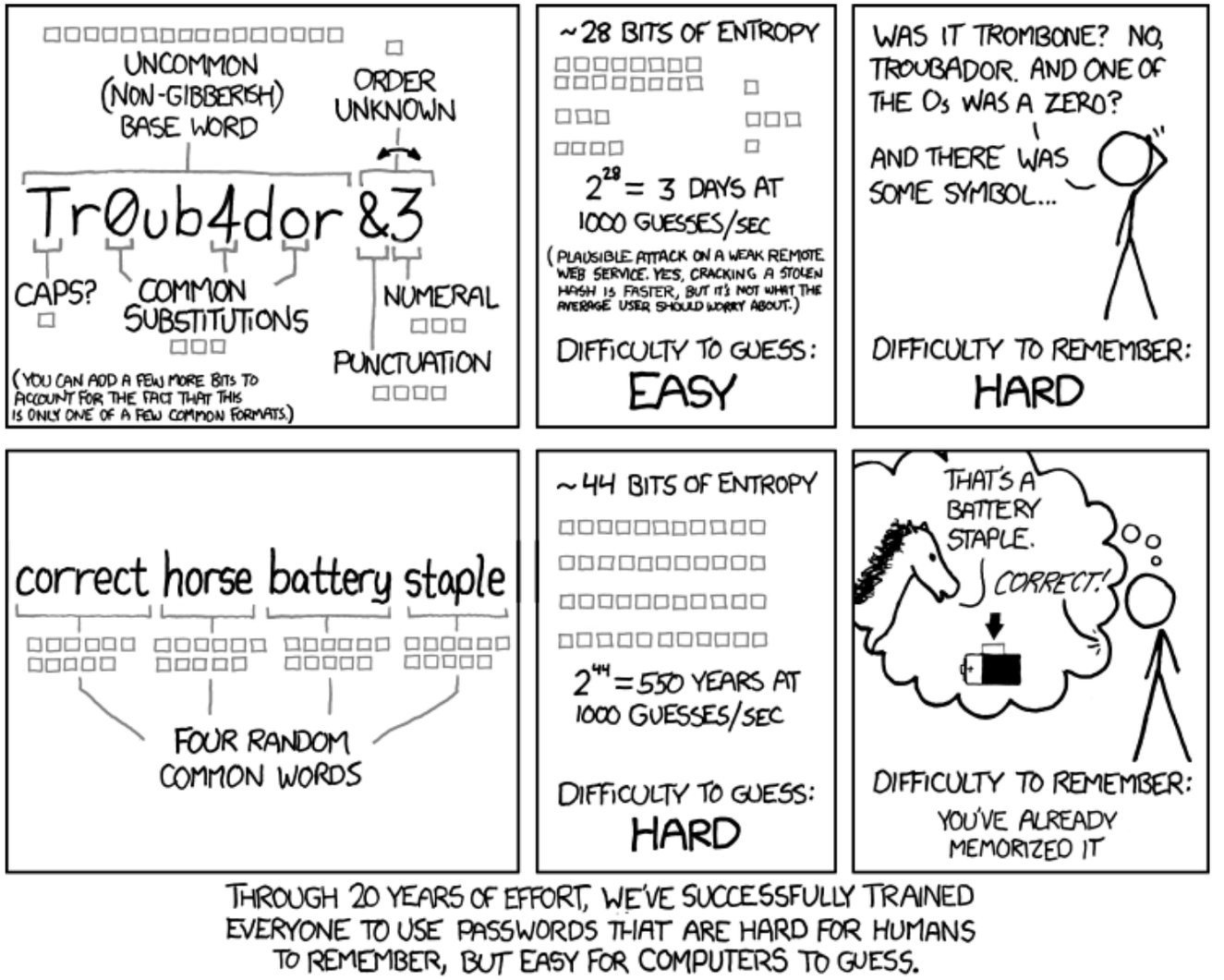
Bewusstsein für Sicherheit schaffen

Sinnvolle Passwort-Beschränkungen

Länge & Zeichensatz

Komplexität

Projekte/APIs wie Telepathwords



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

Weitere Informationen

- Peter.Kirchner @Microsoft.com
- blogs.msdn.com/pkirchner
- Twitter: @peterkirchner

Microsoft Azure
30 Tage kostenfrei testen
bit.ly/AzureAnmeldung

Startseite von Microsoft Azure
azure.microsoft.com

Office 365 testen
www.office.com

© 2013 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries.
The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.