Cyber Risk

Die dunkle Seite des Internets

Marcello Bellini

26.09.2018

Basler Versicherungen

Basler Versicherung und Baloise Bank SoBa

› Generalagentur Luzern

› Hauptsitz Basel

Cyber-Risiken
Die Bedrohungslage

NACHGEFRAGT

Cyber-Attacke auf Altersheim in Schöftland: Woher kam der Erpressungs-Trojaner?

von Nadja Rohner – az Aargauer Zeitung

Pascal Hüsser, Chief Information Security Officer bei der Lenzburger Xint AG, erklärt, wie es zum Hackerangriff auf das Altersheim Schöftland kommen konnte.

© Mario Fuchs/ZVG

Nachdem Hacker das Alterszentrum Schöftland attackiert haben und das Heim erpressten, ermittelt nun die Kantonspolizei. Die AZ hat beim Sicherheitsexperten Pascal Hüsser nachgefragt, wie es überhaupt so weit kommen konnte.

Digitec-Galaxus informiert Kunden über Datenklau

von S. Spaeth - Die Behörden haben kürzlich über 21'000 gestohlene E-Mail-Login-Daten informiert. Nun wird klar: Hacker konnten damit auch auf Kunden-Konten von Digitec-Galaxus zugreifen.

Blick

Home News Sport Politik Wirtschaft People Leben Digital Auto VR Video Services

Europaweite Cyber-Attacke

Russische Hacker greifen Schweizer Olympia-Unternehmen an

Gestern wurde ein Hacker-Angriff auf deutsche Regierungsstellen publik. Auch in der Schweiz sind Unternehmen im Bereich des olympischen Sports betroffen.

20 minuten

Schweiz Ausland Wirtschaft Sport People Entertainment Digital

Zürich Bern Basel Zentralschweiz Ostschweiz Energy Challenge

Hacker stehlen Daten von Schweizer Schuldnern

Bei der Inkassofirma EOS kamen Daten von zehntausenden Personen in fremde Hände. Darunter sind auch Krankenakten.

Die Diebe hatten durch ein schwerwiegendes Datenleck Zugang zu den Firmenunterlagen.

Hackern ist es gelungen, Daten des Inkassounternehmens EOS zu klauen. Durch ein schwerwiegendes Leck bei der Schweizer Tochterfirma konnten sich die Diebe Zugang zu Kreditkartenabrechnungen und Krankenakten verschaffen, wie die «Süddeutsche Zeitung» berichtet. Sie ist durch einen Informanten in den Besitz der Daten gekommen.

Betroffen seien zehntausenden Schuldner aus der Schweiz. In den Daten habe es detaillierte Berichte über ärztliche Behandlungen, Ausweise, Telefonnummern und Adressen. Auf Anfrage der deutschen Zeitung heisst es beim Unternehmen, dass man eine umfassende Revision der Prozesse angeordnet habe. Man habe im April bemerkt, dass ungewöhlich viele Pakete an fremde Computer gesendet werden sollten.

Umfrage

Haben Sie dieses Jahr alle Rechnungen bezahlt?

- Ja, ich zahle immer sofort.
- Ja, hoffentlich habe ich keine Rechnung vergessen.
- Nein, mir fehlt das Geld dazu.
- Nein, bestimmte Rechnungen bezahle ich aus Prinzip nicht.

Abstimmen

Warum Krankenakten erhoben werden, ist unklar

KASPERSKY DAILY

Hackingangriff auf New Yorker Wahrzeichen

New York City ist einer dieser Orte, zu dem Menschen aus aller Welt pilgern. In der Weihnachtszeit gehört ein Besuch der Radio City Music Hall und des Weihnachtsbaums am Rockefeller Center zur jährlichen Tradition vieler Familien. Vergleichbar ist der Madison Square Garden, der für Fans von Sportveranstaltungen und Konzerten ein Leuchtfeuer ist.

Leider sind diese Veranstaltungsorte ins Visier von einigen weihnachtsfeindlichen Hackern geraten. Anfang dieser Woche gaben die Eigentümer vom Madison Square Garden, der Radio City Music Hall und dem Beacon Theater bekannt, dass sie zu Opfern eines Datenlecks geworden waren.

Der Vorfall ereignete sich zwischen November 2015 und Oktober dieses Jahres. Es heißt, dass Hacker persönliche Informationen von Bankkarten stahlen, die an Kassständen verwendet wurden.

In einer Anfrage der NY Daily News sagte das Unternehmen, dass „MSG erkennt, wie wichtig der Schutz unserer Gäste ist und die Unannehmlichkeiten bedauert, die den Kunden dadurch entstanden

Ruag-Hacker haben 20 Gigabyte Daten entwendet

Das VBS hat vorläufige Erkenntnisse zum Cyber-Spionage-Angriff auf die Ruag bekannt gegeben – und bestätigt das befürchtete Datenvolumen.

Die Ruag wurde Opfer eines Hackerangriffs. Ein Mann am Laptop. (Symbolbild)
Bild: Gaetan Bally/Keystone

23.05.2016

Beim Cyber-Spionage-Angriff auf den bundeseigenen Rüstungskonzern Ruag sind mehr als 20 Gigabyte Daten entwendet worden. Darunter dürften auch Daten aus dem sogenannten Admin-Verzeichnis sein, nicht jedoch private persönliche Daten.

Die laufende Untersuchung versuche das abgeflossene Datenvolumen zu rekonstruieren, heisst es in einer Mitteilung des Departementes für Verteidigung, Bevölkerungsschutz und Sport (VBS). Die Wahrscheinlichkeit sei hoch, dass darin Daten aus dem sogenannten Admin-Directory, welches das Outlook der Bundesverwaltung speist, enthalten sind.

Vermutlich Wirtschaftsspionage

Vive les Soldes !

Artikel zum Thema

CVP fordert Klärung beim Cyber-Angriff auf die Ruag

Der Hackerangriff auf den bundeseigenen Rüstungskonzern bewegt die CVP. Sie hat eine dringliche Interpellation eingereicht.

Bund war wohl das Ziel der Ruag-Hacker

Laut dem Rüstungskonzern Ruag sind bei dem verübten Hacker-Angriff nur Daten des

Auswirkungen von Cyber Angriffen

- 60 Firmen aus der Schweiz
  - 26 Firmen > 5000 Mitarbeiter
  - 34 Firmen < 5000 Mitarbeiter

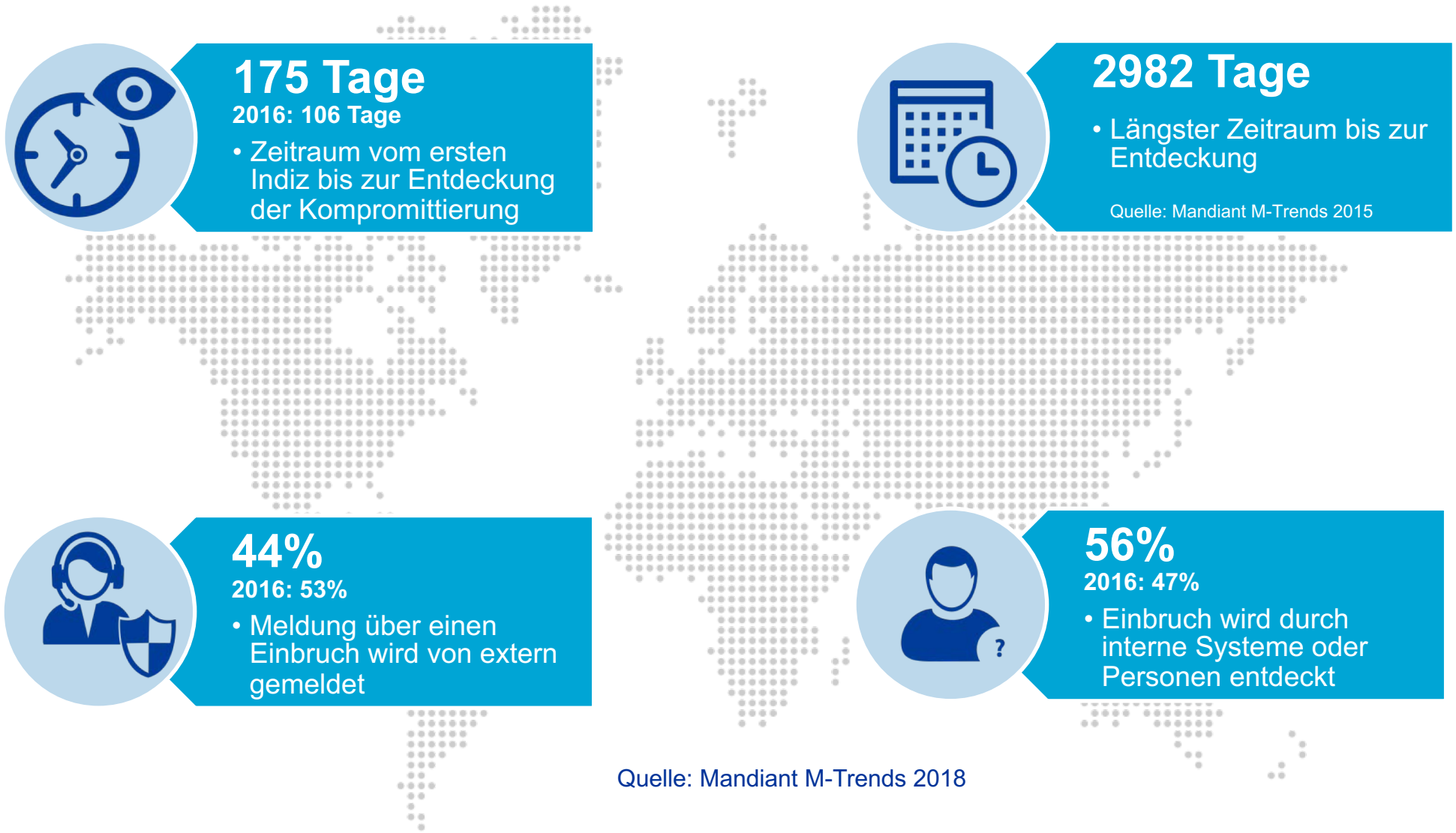
80%

der Geschäftsleitungen sehen Cyber-Security als operationelles Risiko

56%

haben das Budget für Cyber-Security erhöht

Top Facts - Threat Report 2018



175 Tage

2016: 106 Tage

- Zeitraum vom ersten Indiz bis zur Entdeckung der Kompromittierung

2982 Tage

- Längster Zeitraum bis zur Entdeckung

Quelle: Mandiant M-Trends 2015

44%

2016: 53%

- Meldung über einen Einbruch wird von extern gemeldet

56%

2016: 47%

- Einbruch wird durch interne Systeme oder Personen entdeckt

Quelle: Mandiant M-Trends 2018

Equifax Data Breach

143 Millionen Amerikaner betroffen

- Sozialversicherungsnummern
- Geburtsdaten
- Adressen
- Führerscheindaten
- Kreditkartennummern

Angreifer sind über eine Web-Applikation Mitte Mai eingedrungen

- Update für die Schwachstelle war seit März vorhanden

Auswirkungen

Kursverlust 25%

Top Management "in den Ruhestand" versetzt

Hacker knacken Zahlungs-Software

Bei Berner Firma verschwanden 1,2 Millionen Franken

BERN - Hacker haben über Nacht 1,2 Millionen Franken von den Konten der Berner Küng Holding abgezweigt. Firma, Banken und Software-Vertreiberin streiten darum, wer schuld ist.

WannaCry

230 000
Computer in
150 Ländern

Telefonica
NHS
FedEx
Renault
Deutsche Bahn

Was ist das Darknet?

- Public Web
- Deep Web
- Dark Web (Darknet)

From: Armada Collective

Subject: DDOS ATTACK!!!

Date: Wed, 9 Mar 2016 XX:XX:XX +0000

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.

http://www.govcert.admin.ch/blog/14/armada-collective-blackmails-swiss-hosting-providers

All your servers will be DDoS-ed starting Monday (March 14) if you don't pay protection - 25 Bitcoins @ 17j7onEtLgS2pd6qLekKQCteqTrnAFXZV8

If you don't pay by Monday, attack will start, price to stop will increase to 50 BTC and will go up 20 BTC for every day of attack.

This is not a joke.

Our attacks are extremely powerful - sometimes over 1 Tbps per second.

So, no cheap protection will help.

Prevent it all with just 25 BTC @ 17j7onEtLgS2pd6qLekKQCteqTrnAFXZV8

Do not reply, we will not read. Pay and we will know its you. AND YOU WILL NEVER AGAIN HEAR FROM US!

Bitcoin is anonymous, nobody will ever know you cooperated.

Ihre Story, Ihre Informationen, Ihr Hinweis? feedback@20minuten.ch

Armada Collective

16. März 2016 18:32; *Akt: 17.03.2016 00:02*

Schweizer Unternehmen liess sich erpressen

von T. Bolzern - Bei mehreren Schweizer Banken sind DDoS-Erpresserschreiben eingegangen. Um einer Attacke zu entgehen, hat mindestens ein Unternehmen 10'000 Franken bezahlt.

1|4 Bei mehreren Schweizer Banken sind Erpressermails eingegangen. Der Absender gibt sich als sogenanntes Armada Collective aus. (Symbolbild)

Bild: AFP/Michael Bacchiani

ASHLEY MADISON®

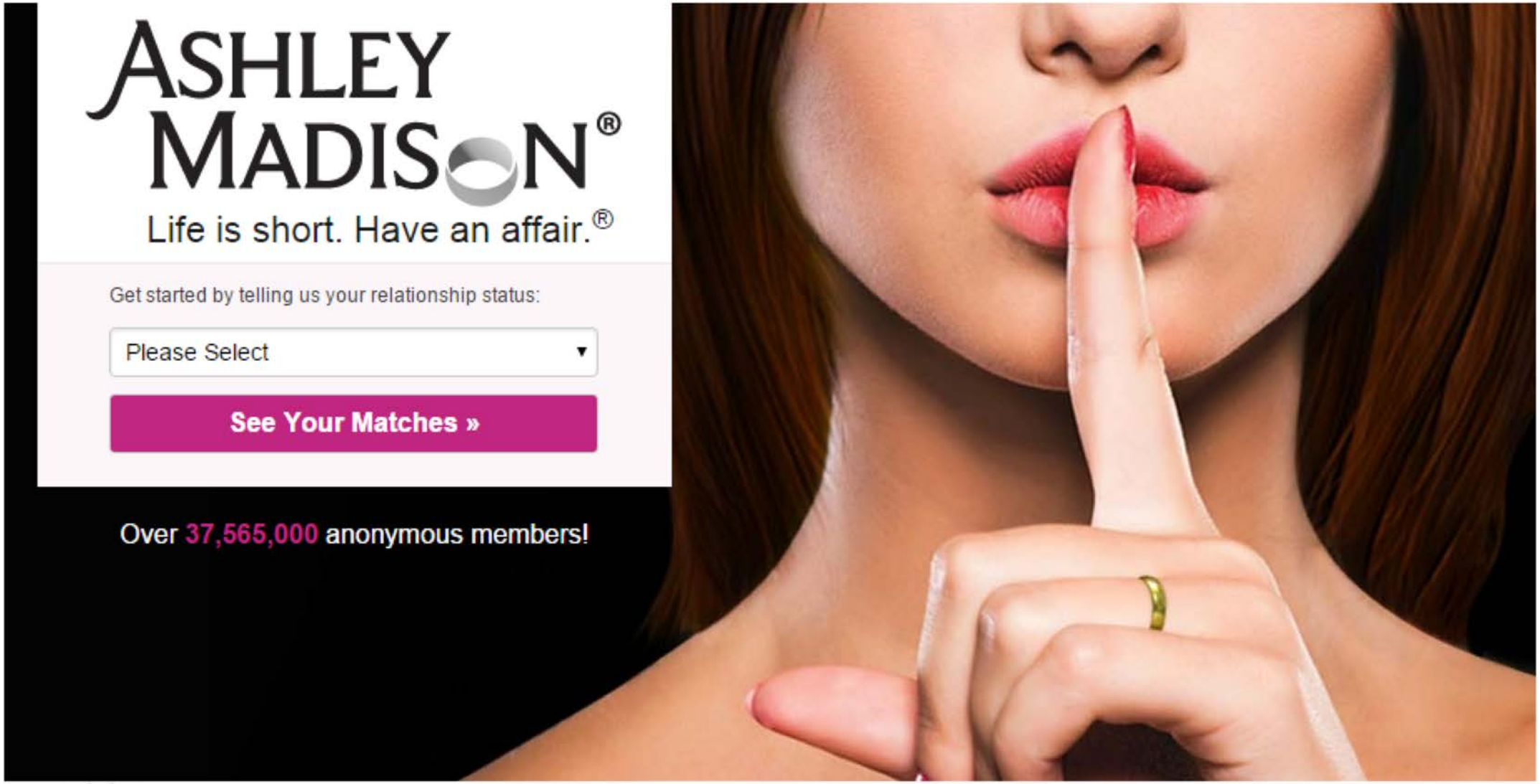
Life is short. Have an affair.®

Get started by telling us your relationship status:

Please Select

See Your Matches »

Over 37,565,000 anonymous members!



★★★★
100%
Like-minded People

As seen on: Hannity, Howard Stern, TIME, BusinessWeek, Sports Illustrated, Maxim, USA Today

Ashley Madison is the world's leading married dating service for ***discreet*** encounters

Trusted Security Award

100% DISCREET SERVICE

SSL Secure Site

AM AND EM MUST SHUT DOWN IMMEDIATELY PERMANENTLY

Avid Life Media runs Ashley Madison, the internet's #1 cheating site, for people who are married or in a relationship to have an affair. ALM also runs Established Men, a prostitution/human trafficking website for rich men to pay for sex, as well as cougar life, a dating website for cougars, man crunch, a site for gay dating, swappernet for swingers, and the big and the beautiful, for overweight dating.

Trevor, ALM's CTO once said "Protection of personal information" was his biggest "critical success factors" and "I would hate to see our systems hacked and/or the leak of personal information"

Well Trevor, welcome to your worst fucking nightmare.

We are the Impact Team. We have hacked them completely, taking over their entire office and production domains and thousands of systems, and over the past few years have taken all

Ashley Madison First Release

Courtesy of Impact Team

Mirrored by TheCthulhu

Or click here to download the torrent (recommended)

File	Signature	File Size	SHA1	SHA256
74ABAA38.txt	None	3 KB	a884c4fcd61e23aecb80e1572254933dc85e2b4a	5e922efe97dc04e1a5cb8d31ed6cdc4cc8354e17d51ccbedf06b78699cce
am_am.dump.gz	am_am.dump.gz.asc	2790 MB	e0020186232dad71fcf92c17d0f11f6354b4634b	6de24a826fdf9edd3569f63ce37c527768532a7070595d429bafc663441f
aminno_member.dump.gz	aminno_member.dump.gz.asc	3259 MB	bc60db3a78c6b82a5045b797e6cd428f367a18eb	e59c8e7e1ba41c26c5a0fcc74b0fdb1a83781770ef2c729752815a892063
aminno_member_email.dump.gz	aminno_member_email.dump.gz.asc	459.8 MB	ab5523be210084c08469d5fa8f9519bc3e337391	70a68e18606d42ba187d7b4f75a7432baa27d3b6360c622e758bc3b41fe
ashleymadisondump.7z	ashleymadisondump.7z.asc	37.8 MB	26786cb1595211ad3be3952aa9d98fbe4c5125f9	7510c8405d9b7497f184bab3b5ef71607348e18b51c8f03634f296a7a6a4
CreditCardTransactions.7z	CreditCardTransactions.7z.asc	290.4 MB	0ad9c78b9b76edb84fe4f7b37963b1d956481068	24f1e25c2c046caa4d3f0a18766f8dd53f372593fb9a3f0a35bf3502680e2
member_details.dump.gz	member_details.dump.gz.asc	738 MB	b4849cec980fe2d0784f8d4409fa64b91abd70ef	3c6f0e178bad9b6814f4eafd2f5197cd8218abe1ca84c8d9ea4ca0003c728

From: "Laura" <....@......xyz>
Subject: You got.... busted

Unfortunately your data was leaked in the recent hacking of Ashley Madison and I know have your information. I have also used your user profile to find your Facebook page, using this I can now message all of your friends and family members.

If you would like to prevent me from sharing this dirt info with all of your friends and family members (and perhaps even your employers too?) then you need to send 1 bitcoin to the following BTC address.

Bitcoin Address:
?????????

You may be wondering why should you and what will prevent other people from doing the same, in short you now know to change your privacy settings in Facebook so no one can view your friends/family list. So go ahead and update that now (I have a copy if you dont pay) to stop any future emails like this.

You can buy bitcoin using online exchanges easily. If the bitcoin is not paid within 3 days then my system will automatically message all of your friends and family members. The bitcoin address is unique to you.

Consider how expensive a divorce lawyer is. If you are no longer in a committed relationship then think about how this will affect your social standing amongst family and friends. What will your friends and family think about you?

Sincerely,
Laura

[CHEAP] DDOS Service [2$ /Per Hour] Thread Options

12-01-2011, 02:34 PM (This post was last modified: 12-23-2011 06:57 PM by [redacted].) Post: #1

[redacted]

ddosdoesnotexist...

Posts: 280
Joined: Sep 2011
Vouch: 0

CHEAP PROFESSIONAL DDOS SERVICE

Cheap Professional DDOS Service
Trusted
Strong/Fast Service
Takes down Large Website/Forum/Game Servers etc.
No time limit

PRICE

1 - 4 hours / 2$ per hour
12 - 24 hours / 4$ per hour
24 - 72 hours / 5$ per hour
1 month / 1000$ fix price

PAYMENT ACCEPTED

Paypal (Verified users only)
Liberty Reserve
Western Union

BitPharma

PRODUCTS FAQS REGISTER LOGIN

Stimulants

Uncut Cocaine and Speed!

Product	Price	Quantity
1g pure Cocaine	85 EUR = 0.242 ฿	1 X Buy now
2g pure Cocaine	160 EUR = 0.456 ฿	1 X Buy now
5g pure Cocaine	375 EUR = 1.069 ฿	1 X Buy now
25g pure Cocaine	1375 EUR = 3.920 ฿	1 X Buy now
10g pure Speed	90 EUR = 0.257 ฿	1 X Buy now

The cards have balances between 800 and 1300 USD or EUR depending on weather you get a chipped card or plain magnetic stripe card.

If you're ordering within the US, regular magnetic cards will work fine, if you're ordering out of any european country we advise you buy our chipped cards as chipped cards are required for authorization in all european countries and many others.

The price brackets(discounts) for the cards are below, if you wish to order more than 20 cards, just ask and we'll give you a price.

MAGNETIC CARDS

(1) One Card	$110 USD
(3) Three Cards	$290 USD
(5) Five Cards	$440 USD
(10) Ten Cards	$790 USD
(20) Twenty Cards	$1390 USD

CHIPPED CARDS

(1) One Card	$145 USD
(3) Three Cards	$380 USD
(5) Five Cards	$575 USD
(10) Ten Cards	$1040 USD
(20) Twenty Cards	$1870 USD

Products | Login | Register | FAQs

UK Passports

Your UK Passport - Name of your choice!

We are selling original UK Passports made with your info/picture.
Also, your info will get entered into the official passport database.
So its possible to travel with our passports.
How we do it? Trade secret!
Information on how to send us your info and pictures will be given after purchase!

You can even enter the UK/EU with our passports, we can just add a stamp for the country you are in!
Ideal for people who want to work in the EU/UK.

Product	Price	Quantity
Your original UK passport with your info/pictures	2000 GBP = 7.493 ฿	1 X Buy now


http://www.fastandeasyhacking.com
ARMITAGE
FAST AND EASY HACKING

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address

pwned?

Generate secure, unique passwords for every account

Learn more at 1Password.com

Why 1Password?

309	5,415,436,787	78,293	85,476,678
pwned websites	pwned accounts	pastes	paste accounts

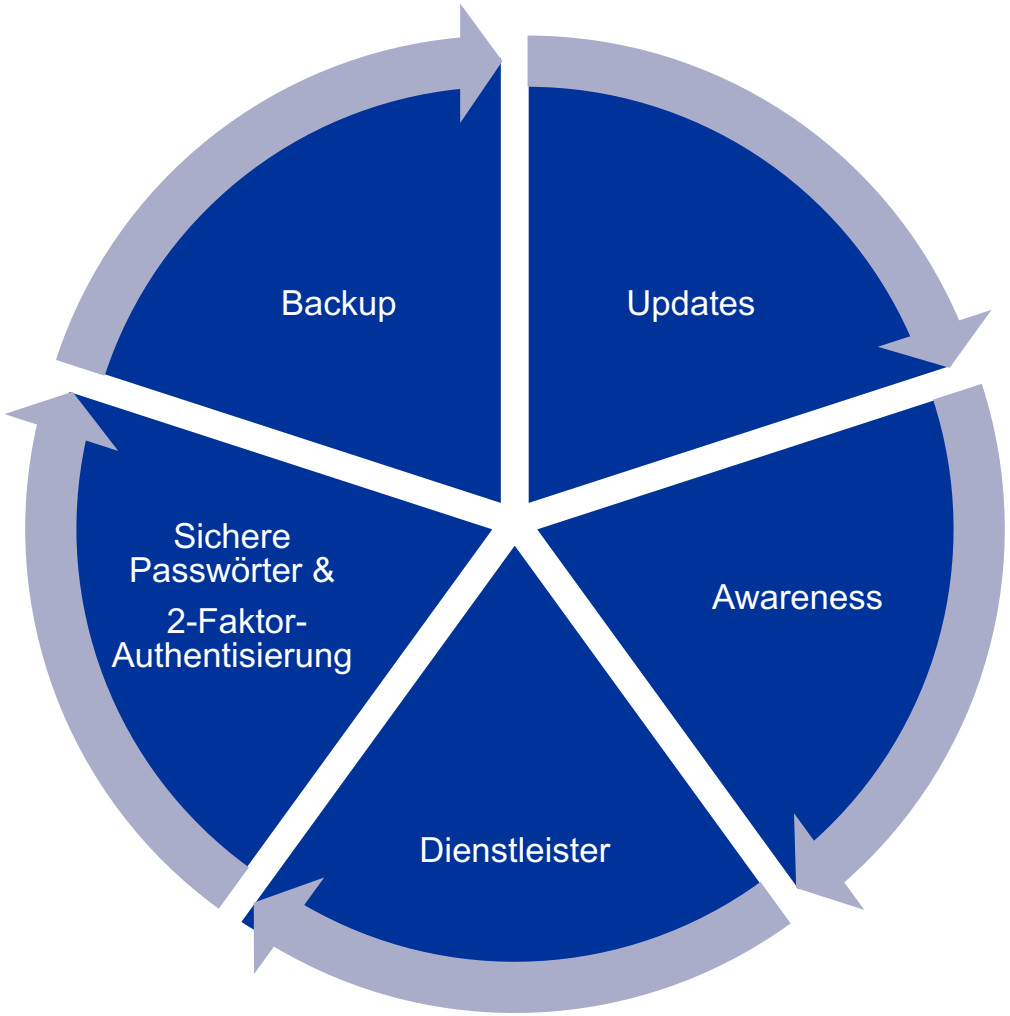
Largest breaches

- 711,477,622 Onliner Spambot accounts
- 593,427,119 Exploit.In accounts
- 457,962,538 Anti Public Combo List accounts
- 393,430,309 River City Media Spam List accounts

Recently added breaches

- 41,826,763 Kayo.moe Credential Stuffing List accounts
- 182,717 Russian America accounts
- 110,355 FreshMenu accounts
- 287,071 NapsGear accounts

Wie kann man sich schützen?



Baloise KMU Cyber-Versicherung

Basler Versicherungen

Vielen Dank für die Aufmerksamkeit!

Marcello Bellini
IT Security Manager

+41 58 285 7394
marcello.bellini@baloise.ch

Basler Versicherungen