Synergie ZKB, GDPR a eIDAS

Workshop ICTU ke kybernetické bezpečnosti a GDPR s následnou diskusi

Ing. Václav Mach

Government and Corporate Affairs, Microsoft Central and Eastern Europe
Přednášející – krátké představení se úvodem
Trocha historie nikoho nezabíjí
A Cloud for **Global Good**

**Fourth** industrial revolution
Fourth industrial revolution

All powered by the cloud
Technology is disrupting everything
An **INVISIBLE** revolution is coming
According to a study, how many items are added to the Internet each second?

127
Nové příležitosti ...
... ale také nové bezpečnostní výzvy?
Synergie mezi IoT vs ZKB, GDPR a eIDAS
IoT & Cybersecurity

Already here...

Coming soon...

DON'T CARE!

DON'T CARE!

Microsoft CityNext

Microsoft Corporation (c) 2017
IoT & Cybersecurity

1. Increasing attack surface
2. Real-world impact
3. New privacy issues
4. IoT
   Cloud
   Big Data
Nařízení – nikoliv směrnice. Je přímo aplikovatelné ve všech zemích EU.

Výhody pro Cloud při GDPR

PŘESUNUTÍ ČÁSTI ODPOVEDNOSTI NA ZPRACOVATELE

1. Ochrana dat (úvěrnost, integrita)
   - Ochrana dat v uložišti a při přenosu

2. Zabezpečení koncových zařízení
   - Zabezpečení zařízení, informací a uživatel identit

3. Řízení přístupu, zabezpečení identit
   - Správa identit v cloudových službách s integrací do on-premise snižuje rizika slabých hesel

4. Nástroje pro kontrolu a auditovatelnost
   - Kontrola pomocí certifikací a auditů třetích stran, provozní logy a další kontrolní nástroje.

5. Nástroje pro vysokou dostupnost a odolnost

6. Zvýšení bez. incidentů
   - Brzká detekce bezpečnostních incidentů, Threat Intelligence
“I don’t think we should wait next 20 years until this thing is fully operational, before we will start making new public policy. But I think we can also not wait 20 months. We have to act now!”

Václav Mach
U.S.: EUROPEAN PRIVACY RULING THREATENS BUSINESS

Max Schrems | Privacy Activist
How can they get your data?

An internet governed by law

Too Important to Fail – Advancing Digital Values
A Principled Approach
Public Safety

Personal Privacy and Free Expression
Respect for National Sovereignty

Open Markets and Global Network
A Cloud for **Global Good**

A roadmap for a trusted, responsible, and inclusive cloud
Inclusive

A cloud for good

Responsible

Trusted
A Cloud for **Global Good**

**Trusted • Responsible • Inclusive**
Policy considerations and recommendations

- A trusted cloud
  - Personal privacy
  - Government access to data
  - Cross-border data flows
  - Secure and reliable cloud services
  - International cybersecurity norms
  - Modern cybercrime prevention

- A responsible cloud
  - Balancing human rights and public safety
  - Technology fraud and online exploitation
  - Environmental sustainability
  - Artificial intelligence

- An inclusive cloud
  - Affordable and ubiquitous access
  - Digital literacy
  - Developing next generation skills
  - Including people with disabilities
  - Supporting businesses of every size
Trusted cloud

A Cloud for Global Good

Personal privacy
Government access to data
Cross-border data flows
Secure and reliable cloud services
International cybersecurity norms
Modern cybercrime prevention
Trusted cloud

- Personal privacy
- Government access to data
- Secure and reliable
- Modern cybercrime approaches
- International security norms
- Cross-border data flows
Modern cybercrime approaches
EU-US PRIVACY SHIELD
Microsoft is first cloud service provider on US list of Privacy Shield-certified entities

Microsoft is the first global cloud service provider to appear on the U.S. Department of Commerce’s list of Privacy Shield-certified entities as of Aug. 12, 2016, writes Alice Rison, Microsoft Azure senior director.

The European Commission adopted the EU-US Privacy Shield Framework on July 12, 2016, replacing the International Safe Harbor Privacy Principles as the mechanism for allowing companies in the European Union and the U.S. to transfer personal data across the Atlantic.
Policy recommendations

Government access to data
Apple Legal Challenge

In early 2016, Apple was presented with an order under the All Writs Act of 1789 to assist law enforcement in unlocking a customer iPhone in San Bernardino, CA. The case is a reminder of the need to develop "21st-century laws that address 21st-century technology issues." Microsoft joined Amazon, Box, Cisco, Dropbox, Evernote, Facebook, Google, Mozilla, Nest Labs, Pinterest, Slack, Snapchat, WhatsApp and Yahoo in filing a join amicus brief in support of Apple in the case.
Microsoft fights warrant for customer emails stored overseas

By James O'Toole @jotoole
Microsoft fights warrant for customer emails stored overseas

by James O'Toole   @jotoole  
June 11, 2014: 2:41 PM ET

Microsoft is fighting a government search warrant seeking customer emails stored abroad in a case that could have far-reaching implications for how tech companies deal with law enforcement.

In a court filing made public this week, Microsoft (MSFT, Tech30) argued that prosecutors had no right to execute the warrant because it seeks information stored at a facility in Dublin, Ireland. The identity of the customer or customers involved isn't clear, though the case relates to alleged drug trafficking and money laundering.

Allowing the warrant to move forward, Microsoft argues, "would violate international law and

international law and treatises, and reduce the privacy protection of everyone on the planet."
Microsoft just won a big privacy fight with the government. Here's what that means.

By Henry Farrell  July 15 at 11:30 AM

Over the past couple of years, the U.S. government and Microsoft have been fighting a legal battle over whether Microsoft has to provide customers’ email that is stored on company servers located in Ireland. On Thursday, a federal appeals court ruled against the government, saying Microsoft was under no legal obligation to provide the data.

[Microsoft just won a huge legal victory on email privacy]

This case has been very closely watched, as it has very important implications for how the U.S. legal system deals with a world where data moves easily across borders.

Jennifer Daskal is an assistant professor at American University’s Washington College of Law. I asked her to explain the issues at stake in the case, and what is likely to happen next.

The U.S. government lost its court battle Thursday to force Microsoft to hand over data from a foreign server. (Zoltan Mathe/European Pressphoto Agency)
A Good Week for Microsoft, a Great One for the Cloud

by Jeff John Roberts  @jeffjohnroberts  JULY 15, 2016, 8:30 AM EDT

The news is full of warnings that our political and economic systems are broken. But that doesn’t mean everything is off the rails. Consider two events this week where judges and regulators got it right, and made critical decisions that will benefit both companies and consumers in the long run.

The first was a thunderbolt decision in which a unanimous appeals court in New York ruled the U.S. government can’t use a domestic warrant to force Microsoft ( msft ) to turn over emails stored on servers in Ireland. The ruling
“U.S. government search warrants cannot compel Microsoft to turn over customer data that is stored exclusively outside the United States.”
OUR LEGAL CHALLENGE TO A U.S. GOVERNMENT SEARCH WARRANT

On July 14, 2016 the Second Circuit ruled 3-0 in favor of Microsoft’s lawsuit challenging a U.S. search warrant for customer emails in our Irish data center. Learn more about how this decision protects people’s privacy rights, helps ensure that information stored in the cloud receives the same protection as physical information, and paves the way for modern solutions that enhance both privacy and public safety. MORE

BLOG

July 14, 2016
Our search warrant case: An important decision for people everywhere
We obviously welcome today’s decision by the United States Court of Appeals for the Second... MORE

April 14, 2015
Keeping Secrecy the Exception, Not the Rule
This morning we filed a new lawsuit in federal court against the United States government... MORE

VIDEO

January 20, 2015
The Search Warrant Case: Consequences for Digital Privacy
Watch the highlight video from the Dec 15 event featuring panelists from legal, media, academic and civil society organizations.

LATEST NEWS

July 14, 2016
Microsoft Wins Landmark Appeal Over Seizure of Foreign Emails

July 14, 2016
Microsoft Just Won a Huge Legal Victory On Email Privacy

MORE
Twice a year we publish the number of legal demands for customer data that we receive from law enforcement agencies around the world. While this report only covers law enforcement requests, Microsoft follows the same principles for responding to government requests for customer data.

Government requests for customer data must comply with applicable laws. A subpoena or its local equivalent is required to request non-content data, a court order or warrant, or its local equivalent, is required for content data.

Read more about Microsoft’s recommendations for continuing to improve transparency, accountability and the balance between personal privacy and public safety.
Microsoft updates biannual reports on our Transparency Hub

Global

Requests

Total number of requests

35,572

Accounts/users specified in request

38,366

Disclosures

% Disclosed content

12.78%

% Only subscriber/transactional data

2.65%

% No data found

18.66%

% Rejected

65.91%

http://blogs.microsoft.com/on-the-issues/2016/09/29/microsoft-updates-biannual-reports-transparency-hub/#sm.01kf1jdm1e4zcwa10zx13yqiqyon0
Global Government Surveillance Reform

The undersigned companies believe that it is time for the world’s governments to address the practices and laws regulating government surveillance of individuals and access to their information.

While the undersigned companies understand that governments need to take action to protect their citizens' safety and security, we strongly believe that current laws and practices need to be reformed.

Consistent with established global norms of free expression and privacy and with the goals of ensuring that government law enforcement and intelligence efforts are rule-bound, narrowly tailored, transparent, and subject to oversight, we hereby call on governments to endorse the following principles and enact reforms that would put these principles into action.
Policy recommendations

Cross-border data flows
Policy recommendations

• Promote trade rules that protect cross-border data flows
• Minimize disruptions to data flows in domestic legislation
• Encourage e-commerce
• Avoid establishing conflicting rules that raise barriers
Policy recommendations

Cybersecurity norms
International
cybersecurity norms
Policy recommendations

<table>
<thead>
<tr>
<th>Desired impacts of Microsoft's proposed norms</th>
<th>Cybersecurity norms proposed by Microsoft for nation-states</th>
<th>Cybersecurity norms proposed by Microsoft for the global ICT industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintain trust</td>
<td>States should not target global ICT companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in products and services.</td>
<td>Global ICT companies should not permit or enable nation-states to adversely impact the security of commercial, mass-market ICT products and services.</td>
</tr>
<tr>
<td>Coordinated approach to vulnerability handling</td>
<td>States should have a clear, principle-based policy for handling product and service vulnerabilities that reflects a strong mandate to report them to vendors rather than to stockpile, buy, sell, or exploit them.</td>
<td>Global ICT companies should adhere to coordinated disclosure practices for handling of ICT product and service vulnerabilities.</td>
</tr>
<tr>
<td>Stop proliferation of vulnerabilities</td>
<td>States should exercise restraint in developing cyber weapons and should ensure that any which are developed are limited, precise, and not reusable.</td>
<td>Global ICT companies should collaborate to proactively defend against nation-state attacks and to remediate the impact of such attacks.</td>
</tr>
<tr>
<td>Mitigate the impact of nation-state attacks</td>
<td>States should commit to nonproliferation activities related to cyber weapons.</td>
<td>Global ICT companies should not traffic in cyber vulnerabilities for offensive purposes. If they should ICT companies embrace business models that involve proliferation of cyber vulnerabilities for offensive purposes.</td>
</tr>
<tr>
<td>Prevent mass events</td>
<td>States should limit their engagement in cyber offensive operations to avoid creating a mass event.</td>
<td>No corresponding norm for the global ICT industry.</td>
</tr>
<tr>
<td>Support response efforts</td>
<td>States should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace.</td>
<td>Global ICT companies should assist public sector efforts to identify, prevent, detect, respond to, and recover from events in cyberspace.</td>
</tr>
<tr>
<td>Patch customers globally</td>
<td>No corresponding norm for nation-states.</td>
<td>ICT companies should issue patches to protect ICT users, regardless of the attacker and their motives.</td>
</tr>
</tbody>
</table>

https://mscorpmedia.azureedge.net/mscorpmedia/2016/06/Microsoft-Cybersecurity-Norms_vFinal.pdf
Final conclusion

Devices added to the Internet during the last 30 minutes:

228,600
Evidence and further reading:

**World Economic Forum Report:** “Rethinking Personal Data: Trust and Context in User-Centered Data Ecosystems”

**IPAA Blog:** Ten Steps to a Quality Privacy Program, Part Three: Privacy By Design Tools

**Microsoft Blog:** EU-U.S. Privacy Shield: Progress for privacy rights

For links to these and other resources, please visit: http://www.microsoft.com/cloudforgood
Evidence and further reading:


Microsoft Blog: Keeping secrecy the exception, not the rule: An issue for both consumers and businesses

Lawfare: “Cross-Border Data Requests: A Proposed Framework”

Just Security: “Privacy Rights Advocates Embrace DOJs Cross Border Data Proposal”

The Guardian: “Tech giants reach White House deal on NSA surveillance of customer data”

For links to these and other resources, please visit: http://www.microsoft.com/cloudforgood
Evidence and further reading:


Information Technology & Innovation Foundation: “Cross-Border Data Flows Enable Growth in All Industries”


BSA | The Software Alliance: “What’s the Big Deal with Data?”

For links to these and other resources, please visit: http://www.microsoft.com/cloudforgood