MOSCOW FORENSICS DAY '25



KONSTANTIN TITKOV

"HOW NOT TO END UP NEEDING FORENSICS,
AND WHAT TO DO IF IT CAN'T BE AVOIDED"

MFD

What to do when everything is encrypted and stolen

Konstantin Titkov

Head of subsidiary cybersecurity centre, Gazprombank
Cyberdom ambassador

09.2025

What this talk is about

- What's wrong with the typical IT BCDR plan?
- Emergency actions
- Who can help, and how
- Stages of incident response
- What to do afterwards
- **If personal data leaks**
- How to prepare so it doesn't hurt THAT much

P.S. These recommendations are intended for IT and security teams of SMB and are designed for fast and effective incident response involving an external expert organization, and are not addressed to DFIR (Digital Forensic and Incident Response) or SOC (Security Operations Center) experts of large and the largest companies, since such experts are professionals in their field and are guided in their work by industry-specific recommendations and standards, a small part of which is mentioned in this talk.

P.P.S. The recommendations cannot be absolutely applicable to all possible cases and cannot guarantee a perfect outcome of actions when responding to a security incident.

07.2025, hot on the heels of successful attacks

Target and incident date	Incident, officially	Consequences and recovery
Beverage producer and federal retail chain, 14 July	"... the group suffered an unprecedented cyberattack – a large-scale, coordinated operation carried out by hackers..."	• Financial losses, data loss, reputational damage, customer churn • Recovery: about two weeks, full recovery – a month
Major airline, 27 July	"... owing to a failure in the IT infrastructure the airline is making a forced adjustment to its flight schedule, including by partially cancelling flights..."	• Financial losses, data loss, reputational damage, regulatory inspections, possible liability of officials Recovery: several days, some • functions unavailable
Federal pharmacy chain, 29 July	"We faced a serious technical failure caused by a hacker attack. As a result, the work of the pharmacies was disrupted.."	• Financial losses, data loss, reputational damage, customer churn • Recovery: more than two weeks
Next organization **(date to be confirmed...)**	To be disclosed later	Assessment pending

- ELE-level events are likely (Extinction Level Event), when an organization's activity cannot or should not be restored: total loss of critical production assets, including their physical destruction

- **Critically important: prepare to deal with an attack's aftermath before the attack itself starts**

The main goal – restore operations as soon as possible

- Stopping at this goal alone – a mistake!

What gets forgotten:

- Kick the attacker out
- Find out how they got in
- Prevent repeat intrusion
- Identify all attack consequences
- Minimize the damage
  (customers, counterparties, reputation, fines...)

- “We caught the ransomware!”
  – an incorrect statement



There is a plan, but the wrong one

IT incident: human error or technical failure

- Recovery in a few hours (recovering data and individual IT infrastructure elements is practised and honed)

Security incident: targeted deliberate malicious action on all or any elements of the infrastructure and the personnel, at any time and adaptively – allowing for counter-actions

- **Recovery in several days / weeks**

Time is spent on:
- panic / pointless actions
- making the decision to respond
- incident response
- restoring the IT infrastructure
- restoring data

Friday and public holidays

- An incident is the finale of a chain of events, the last step
- Act immediately, quickly and effectively (even at night)
- **Readiness for an incident matters**
- Rely on your own groundwork and on on-duty staff
- The ability to bring in help – priceless!

(and cheaper than downtime)



No recommendations exist – let's make them!

- Konstantin Titkov, head of subsidiary cybersecurity centre, Gazprombank; Cyberdom ambassador
- Sergey Golovanov, chief expert, Kaspersky Lab JSC
- Anton Velichko, head of the Digital Forensics and Malware Research Lab, F6
- Ilya Zuev, VP for cybersecurity, MTS Bank
- Colleagues who asked questions and shared their experience



How could this even happen?

- VPN, RDP, SSH, OWA, Jira, Confluence, Gitlab, Sharepoint etc. - an unpatched vulnerability or password guessing
- Phishing, including from trusted addresses
- Compromise of trusted relationships
- **WEB application - vulnerability**
- **Supply chain attack**
- Insider threat actor
- And so on...



Should you pay the ransom?



Emergency actions

- Check online banking operations
- **Do not power off and do not reboot**
- Isolate valuables / backups and their media
- **Take “snapshots”**
- Examine the outbound traffic
- **Consider network isolation**
- Arrange the staff's working schedule
- **Support the employees involved**

Who's in charge? And the other responders

- Communications OUTSIDE the affected infrastructure
- **Define realistic goals**
- **Perform DFIR**
- Go to law enforcement
- **Bring in IT contractors**
- Inform customers and partners
- **A “stub page” on the site**

Roles in handling a security incident

- Decision maker
- Work coordinator
- Security
- IT
- Lawyer
- PR/Marketing
- HR

If personal data leaks, also those responsible for:

- personal data processing
- personal data security



Need help?

- Choice of company (-ies), engagement mode, number of experts, date/time
- Address, contacts, passes, parking, letters of guarantee, NDA
- Kick-off meeting
- Analysis of compromised hosts, HDDs (imaging for analysis)
- Search for entry points, all affected hosts and implants (RAT)
- **Report preparation**
- With 2 DFIR experts the mode is 24/7: 8 hours an expert works alone, 8 - together with a partner, 8 for rest.
  Ensure the same working mode!

- Need it faster – need more DFIR experts
  Better discuss timelines and rates before the experts arrive
- NKTsKI (National Coordination Center for Computer Incidents)
  https://www.cert.gov.ru/abuse/

What to prepare?

- Workplaces (desk/chair/light/power/coffee machine...)
- Chat OUTSIDE the corporate messenger with the necessary people (IT, security, management, lawyer, marketing/PR, ...)
- “Silence mode” in the internal network, mail, messengers (if they were logged into from the corporate network)
- Synchronized working hours for IT/security staff and DFIR experts

Cancellation of leave, business trips, resignations

- Compensation for overtime

The chat's confidentiality is critically important!



Stage 1: Preparing for an incident

- Logs – they exist and are secure (scope, location, depth)
- Disks – accessible (find them, hold them, remove protection)
- Artifacts – can be collected (availability, rights, passwords)
- Reserves – sufficient and available
- Backups – complete (data + software) and secure

(and there's what to restore them with and onto!)

Stage 2: Identifying the incident

- Threat Intelligence
- SOC/SIEM
- MDR
- EDR/XDR
- AV
- ...
- IT monitoring system (security tools being disabled)
- ...
- Screen of an encrypted computer (if you didn't bother with the items above)
- Telegram/MAX channels... (if you're on vacation)



Stage 3: Containment

- Do NOT cut the power!
- **Do NOT reboot!**
- BUT disconnect from the LAN:
- Virtual machines
- Physical machines
- Wi-Fi and other interfaces



Stage 4. Cleanup

- Removing trojans/implants/web shells/RAT etc.
- Installing security updates (for entry points + the latest)
- Restoring security tools
- Changing passwords:
  - domain and system accounts. Kerberos – x2
  - and local ones, in DBMS, VPN, applications...
  - and SSH/SSL keys too.
  - and web service certificates.
  - and passwords/keys in your online banking.
  - and in internet services and personal accounts.

  Change ALL passwords, basically!
- Check the list of accounts. Including system ones.



Stages 5-6: Recovery and lessons learned

- Restoring from backups
- Turning interfaces back on



- Report on the incident and the response
- Recommendations to NOT repeat it
- Work plan

Does all this take long?

Rough timeline estimates:

- Ransomware not launched yet? From 2 hours.
- **Analysis of a couple of HDDs – 1 day**
- **100 - 200 hosts - 1 week of work for 1 expert**
- 1000 - 2000 hosts - 2 weeks for 2 experts
- 50,000 - 150,000 hosts - 2 months of work by combined teams

Maybe online?





Online is possible

- Online is possible if you can collect logs, evidence etc.
- The experts will study the data and request what's missing
- Online IR can be cheaper in terms of expert rates

+ no travel and business trip costs!

- BUT: without coordinated, fast and expert work on the client's side DFIR can take longer and even cost more than offline!

Is that all? No, unfortunately...

- Going to law enforcement
- Complaint materials
- DFIR report
- KUSP
- Seizure
- Opening a criminal case
- Certificate recognizing the company as victim
- Dealing with other government bodies



And that's still not all

Theft of information and personal data:

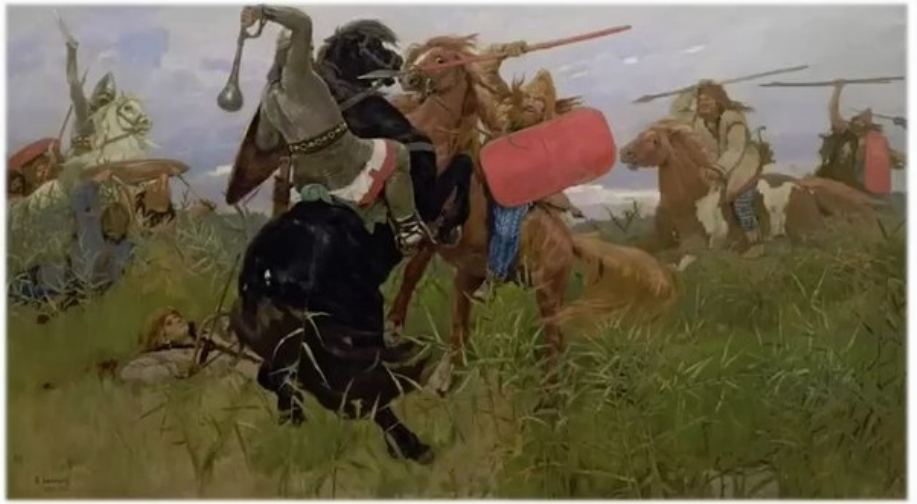
- ransom for deleting it
- selling the data
- publishing the data

- Personal data of employees and customers
- Intellectual property
- Contract terms
- Keys and passwords



In case of a personal data leak

- Enquiries from customers, partners, law enforcement.
- In the future - new parts of data previously stolen from you may be published and passed off as a new leak.
- You must be ready to analyze such data in order to either confirm that it's an old leak, or run DFIR again or a Compromise Assessment (CA).



In case of a personal data leak

So now (and in the future - every time):

- 24 hours - notify Roskomnadzor
- 72 hours - report on the results of the internal investigation
- CII entity - notify NKTsKI within 24 hours (GosSOPKA format)
- Under the Central Bank - ASOI FinCERT
- GDPR (?)



In advance, for each party to be informed

- notification procedure and requirements for data form and content
- primary and backup notification channels

access to personal accounts

account for the branch network of your organization / group / holding

- those responsible for drafting, approving and sending reports
- procedure for informing data subjects about the leak and for posting leak information in open sources

those responsible for drafting, approving and publishing the information

- agree press release templates in advance

Recommendations for reporting on leak response

The report may consist of the following sections:

- Introduction - the date and time the leak information appeared, the composition of the information claimed and the information actually published by the attackers
- Investigation results - circumstances and causes of the leak, composition and volume of the leaked data or of data that could have leaked, whether data subjects' interests may suffer from the leak as projected onto the organization's services, whether the culprits were identified and what measures were taken against them
- Conclusion from the analysis of the leaked data – assessment of its authenticity/fakeness and uniqueness given third-party leaks
- Measures taken - tactical and strategic measures with a detailed description

Better to prepare an exhaustive report!



Got it. Can I have a preventive check-up?

What to do if you suspect that your IT infrastructure has been hacked and may be encrypted/destroyed, but this hasn't happened yet.

What could be such grounds?

- A sense that the IT infrastructure is working incorrectly, for example because of changes made in it with administrative rights that you did not authorize
- Vulnerable software or services on the external (internet) perimeter that you don't fix promptly.
- A penetration test report with a successful compromise of the infrastructure.
- **And much more...**

In this situation it makes sense to:

- run a CA (Comromise Assessment) – searching for traces of a breach
- check the security, integrity and availability of your backups (data backup copies)
- **Prepare for a future incident**

How to prepare? CISO & CIO/CTO

- Develop a response plan for a successful cyberattack with the most dismal consequences
- Create a reserve of equipment, funds etc.
- Pay special attention to the security of data backups and of the software itself (“3-2-1”)
- Protect the backup system
- Response exercises
  + measure the time
- Choose DFIR partners in advance
- If you suspect a breach
  - Comromise Assessment



How to prepare? CEO

- Pass recommendations to IT and security
- Check that everyone can do everything and everyone has everything, the preparatory steps are done
- Estimate the downtime during a security incident
- In an incident, bring in all resources
- Support the employees while the incident's consequences are being dealt with, not punish them



A demotivated employee has no interest in incident response, while an employee who let it happen (their fault or not) but fixed the situation is better and more valuable for your company than a new one!

Recommendations:
https://cyberdom.pro/recomendationbig

CEO quick guide:
https://cyberdom.pro/recomendationceo

Thank you for your attention!

Konstantin Titkov