OTRS Security MINI.CON | Matthias Terlinde | 2019-09-12

STORM and the GDPR

T · · Systems · Let's power higher performance

Introduction

- Matthias Terlinde
  - SOC Analyst at DTAG since 2017
  - OTRS administrator for the SOC and CERT
- Only OTRS specific topics today

GDPR topics

- Not compliant by default
  - Data restriction is the hardest
- Some solutions we found
- A few privacy related wishes for OTRS

GDPR – Obligation to inform

- REST API users aren‘t data subjects
- No need to inform for transit email ←→ OTRS
- Welcome email for agents
  - Especially ticket history
  - Duration of storage
  - Pseudonymization
  - Data subject rights
  - No automated agent analysis

GDPR – Right to Access

- No solution provided for non-agents
  - Full text search to the rescue!
  - No possibility for singular dump
- Agents can view most data

GDPR – Deletion concept

- How long will data be stored?
- How to delete them?
- Deletion logs are needed

GDPR – Deletion concept

- Example (fictional):

Department	Storage duration
SOC	1 year
CERT	5 years
Security Awareness	2 years

- Create Generic Agent
  - Closed tickets
  - Closed before *today – storage duration*
  - Invokes logging script
- Create log rotation for 365 days

GDPR – Deletion concept

loggingScript.sh

```
#!/bin/bash

        logger -i -p local0.info “OTRS GenericAgent deleted ticket number $@”

exit 0
```

GDPR – Deletion concept

/etc/rsyslog.d/50-defaults.conf (partial)

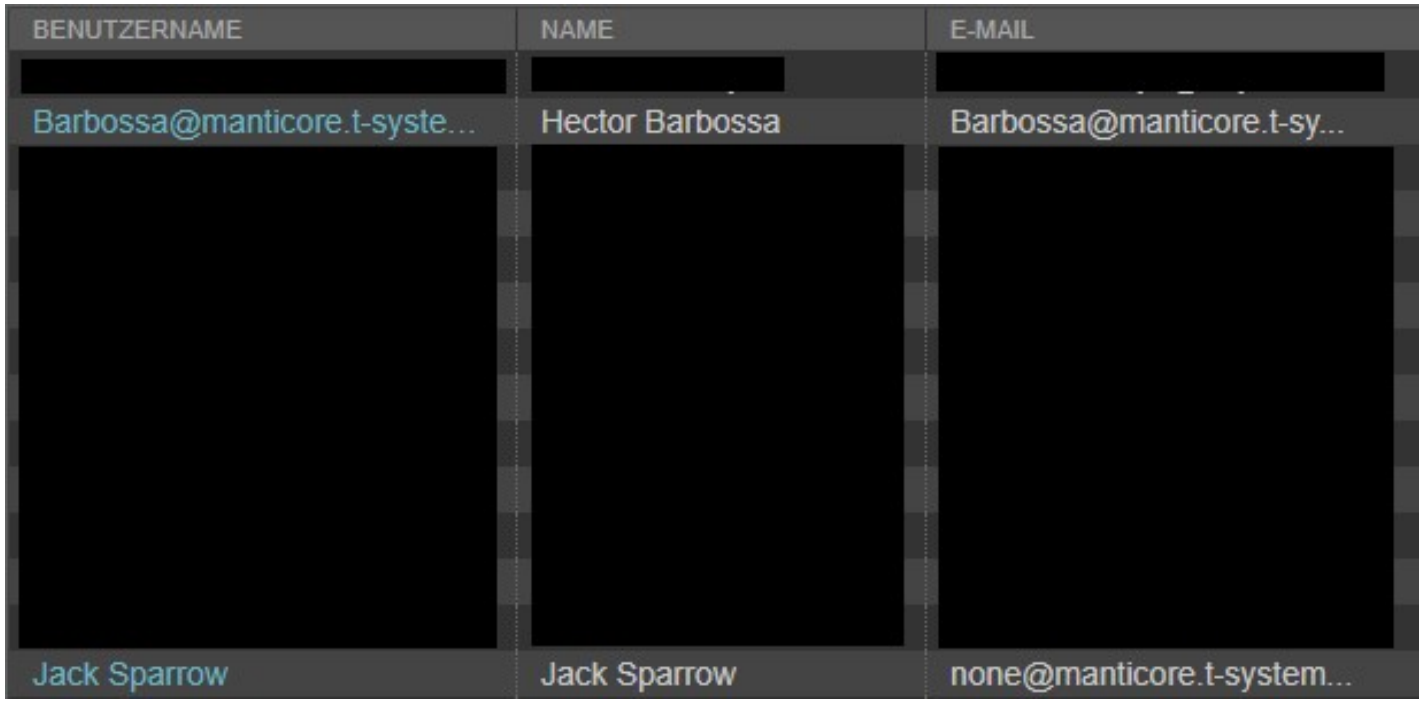
```
auth,authpriv.*                 /var/log/auth.log
*.*;auth,authpriv.none          -/var/log/syslog
kern.*                          -/var/log/kern.log
mail.*                          -/var/log/mail.log
local0.*                        /var/log/otrsDeletion.log
local1.*                        /var/log/otrs.log
```

GDPR – Data minimization

- History entries needed?
- Last login timestamps needed?
- Agents need proper deboarding

GDPR – Deboarding of agents

- User accounts live forever in OTRS
- We change account names during deboarding
- No function to delete account if no ticket is linked to it



GDPR – Restriction of processing

- Data needs restriction if
  - Content is disputable
  - Data subject wants deletion where deletion is not possible

1. Create new queue
2. Move tickets into it
3. Grant permissions
4. Repeat for every occurrence of restriction

GDPR – Logging of PII change

- The logging for agent actions is good (ticket history)
- There is no logging for admin changes
- Deletion log was mentioned before

Feature wishes

- Easy way for data disclosure and data transfer
- Deletion of agent accounts, if there is no linked ticket
- Admin logging of PII changes
- Build in deletion log

Conclusion

Thank you!

Questions?

Matthias.Terlinde@t-systems.com

T · · Systems ·

Let's power
higher performance