Evolution of Password Expiry in Companies: Measuring the Adoption of Recommendations by the German Federal Office for Information Security

Eva Gerlitz¹, Maximilian Häring², Matthew Smith¹,², Christian Tiefenau²

¹: Fraunhofer FKIE, ²: University of Bonn
Motivation

NIST deletes recommendation for password expiry

2013

Research: Password expiry not a good idea

Please do not use !? or your License Plate Number: Analyzing Password Policies in German Companies

Eva Geritz, Fraunhofer FKIE; Maximilian Haring, University of Bonn;
Matthew Smith, University of Bonn, Fraunhofer FKIE

https://www.usenix.org/conference/soups2021/presentation/geritz

2016

2019 2020 2021 2022 2023
Motivation

Research: Password expiry not a good idea

NIST deletes recommendation for password expiry

BSI deletes recommendation for password expiry

2013 2016

2019 2020 2021 2022 2023

70% of German companies use password expiry

How about password policies now?

70% of German companies use password expiry
Methodology of Expert Study

Participants

Asked for:
- Policy
- Password expiry (2023)
- Alternative checks (2023)
Usage of Character Classes (%)
Usage of Minimal Length (%)
Usage of Password Expiry (%)

- **2019**: 
  - ≤ 90
  - > 90
  - No

- **2020**: 
  - ≤ 90
  - > 90
  - No

- **2022**: 
  - ≤ 90
  - > 90
  - No

- **2023**: 
  - ≤ 90
  - > 90
  - No
Usage of Password Expiry (%)

\[ p < 0.01 \]
\[ OR = 4.71 \]
Summary

Minimal length

<table>
<thead>
<tr>
<th>Year</th>
<th>≤ 8</th>
<th>≤ 10</th>
<th>≤ 12</th>
<th>&gt; 12</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2023</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Password expiry

<table>
<thead>
<tr>
<th>Year</th>
<th>≤ 90</th>
<th>&gt; 90</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2023</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Trend to longer minimal length and no password expiry
Elements of password policies

<table>
<thead>
<tr>
<th>Expiry (days)</th>
<th>Min. Len</th>
<th>Complexity</th>
<th>2019</th>
<th>2020</th>
<th>2022</th>
<th>2023</th>
</tr>
</thead>
<tbody>
<tr>
<td>90</td>
<td>8</td>
<td>3</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>90</td>
<td>8</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>90</td>
<td>10</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>180</td>
<td>8</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>180</td>
<td>8</td>
<td>4</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Not mentioned</td>
<td>8</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Not mentioned</td>
<td>8</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Not mentioned</td>
<td>12</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>Not mentioned</td>
<td>12</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>Explicitly not</td>
<td>12</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>4</td>
</tr>
</tbody>
</table>

But: 45% still use password expiry!
Why is password expiry still in use in 2023?

36 answers
Why is password expiry still in use?

Security!

“Because after a year, the risk of misuse of the PW through reuse with other, potentially corrupted services, is too great.”

“... adds ‘some’ security”
Why is password expiry still in use? Requirements!

“Official (in my eyes outdated) requirements in handling officially classified data.”

„Internal policies require this change, contrary to the recommendation of the IT sec [department]“
Why is password expiry still in use? Technically difficult

“… there is currently no other technical solution.”
How do companies check for compromised accounts?

66 answers
Check for compromised accounts

Anomaly detection
16

Leak check
8
No check because …

Difficult 9

Resources 7

Structural 5
Summary

- Password expiry is still a thing.
  - Assumptions that might not hold
  - More hope for improvement than actual improvement
  - Management needs to be convinced
  - Technical issues

We need to find easy solutions for implementing different checks and/or find out why current solutions are not used.

We need to help experts in communicating necessary changes to management
Summary

Password expiry is still a thing, 
- Assumptions that might not hold
- More hope for improvement than actual improvement
- Management needs to be convinced
- Technical issues

We need to find easy solutions for implementing different checks and/or find out why current solutions are not used.

We need to help experts in communicating necessary changes to management

Evolution of Password Expiry in Companies: Measuring the Adoption of Recommendations by the German Federal Office for Information Security

Eva Gerlitz¹, Maximilian Häring², Matthew Smith¹,², Christian Tiefenau²
¹: Fraunhofer FKIE, ²: University of Bonn