

# Pandemie-Monitoring: im Ernstfall gewarnt

Bei einer Grippepandemie muss ein Unternehmen abschätzen können, wie stark es von Absenzen betroffen sein wird. Die Stadtverwaltung Zürich hat dafür ein effizientes Monitoring-Tool entwickelt.

→ VON ULRICH ERLINGER & JEAN-LUC NOTTARIS

Während einer schweren Grippepandemie können die vielen Absenzen für den Geschäftsbetrieb zu einem ernststen Problem werden. Eine verantwortungsvolle betriebliche Pandemieplanung sieht deshalb geeignete Gegenmassnahmen vor, zum Beispiel das Inkrafttreten von Vertretungsplänen. Für Unternehmen mit einer grossen Zahl Abteilungen und vielfältigen Aufgaben ist es jedoch nicht einfach, den drohenden Personalmangel frühzeitig zu erkennen. Dieses Wissen ist aber wichtig, um rechtzeitig mit dem Aufgebot von Mitarbeitenden im Ruhestand zu beginnen oder eine Feriensperre auszusprechen.

Damit die Stadtverwaltung Zürich aussergewöhnliche Absenkraten möglichst schnell erkennen kann, hat der Pandemiestab des Umwelt- und Gesundheitsdepartements (GUD) und die Dienstabteilung Organisation und Informa-

tik der Stadt Zürich (OIZ) ein spezielles Werkzeug entwickelt. Das Monitoring-Tool wertet die täglichen PC-Logins der Mitarbeitenden anonymisiert aus und macht so ausserordentliche Abwesenheiten frühzeitig erkennbar.

## DIE WICHTIGSTEN ANFORDERUNGEN

Die Stadt Zürich beschäftigt rund 24 000 Mitarbeitende in neun Departementen, die sich auf das gesamte Stadtgebiet verteilen. Da die Organisationseinheiten in der Stadtverwaltung auf unterschiedliche Arbeitszeiterfassungssysteme setzen, gab es kein einheitliches Produkt, das als Quelle für die Präsenzinformationen dienen konnte. Eine Konsolidierung der Informationen der unterschiedlichen Produkte wäre wegen der grossen Zahl notwendiger Schnittstellen sehr kostspielig gewesen. Im Pandemiestab entstand deshalb die Idee, die Zahl der täglichen Anmeldungen am Computer als Indi-

kator für ausserordentliche Absenkraten zu verwenden. Annähernd die halbe Belegschaft verfügt über einen Computerarbeitsplatz, was eine gute Stichprobengrösse ergibt.

Das Monitoring-Instrument sollte dabei verschiedene Anforderungen erfüllen: Einerseits mussten die Präsenzinformationen eines repräsentativen Teils der Belegschaft tagesaktuell und weitgehend automatisch verfügbar sein, andererseits sollte aber auch der Datenschutz gewahrt bleiben.

## TECHNISCHE AUSGANGSLAGE

Bei der Entwicklung des Frühwarnsystems konnte das Projektteam auf Komponenten zugreifen, die in der Stadtverwaltung Zürich seit mehreren Jahren im Einsatz sind:

- **Domain Controller:** Das zentrale System, an dem sich ca. 80 Prozent der rund 11 000 PC-Anwender anmelden, ist das von der OIZ betriebene Windows-Verzeichnis. Für die Anmeldevorgänge stehen mehrere Rechner, die sogenannten Domain Controller, im Einsatz. Auf ihnen wird jede Anmeldung registriert und im Security Eventlog gespeichert. Ein Login läuft in mehreren Schritten ab, für die unterschiedliche Ereignisse registriert werden. Dabei hat sich herausgestellt, dass das Windows-Ereignis «EVENT ID 672 Authentication Ticket Granted» am besten geeignet ist.
- **«EventReporter»:** Die Informationen sind über mehrere Computer verteilt und dort nur für

wenige Tage gespeichert. Aus diesem Grund werden diese sicherheitsrelevanten Logs zur Auswertung an ein zentrales System (den Loghost) weitergeleitet. Dazu wird «EventReporter» von Adiscon ([www.adiscon.de](http://www.adiscon.de)) eingesetzt, der – als Dienst auf dem Domain Controller installiert – die Logs laufend weiterleitet.

- **Loghost:** Als Loghost setzt die Stadtverwaltung «tacLOG» von der Schweizerischen terreActive ([www.terreActive.ch](http://www.terreActive.ch)) ein. Hier werden jeden Tag sieben Millionen Ereignisse (Security Events) von den Domain Controllern gezählt, was einem Datenvolumen von rund sieben Gigabyte entspricht. Da auf dem Loghost die Informationen aller Domain Controller zusammengefasst sind, ist dies auch der geeignete Ort, um die Auswertungen für das Absenzen-Monitoring durchzuführen.
- **«Stata9»:** «Stata» ([www.stata.com](http://www.stata.com)) ist eine umfassende, integrierte Statistik-Software für Analysen und grafische Darstellungen. Sie wird im städtischen Dienst verwendet.

## AUSWERTUNG IN ECHTZEIT

Die Zahl der täglichen PC-Anmeldungen wird aus den Aufzeichnungen des Domain Control-

Ulrich Erlinger arbeitet beim Pandemiestab des Gesundheits- und Umweltdepartements Stadt Zürich (GUD). Jean-Luc Nottaris ist für die Fachstelle Informatikssicherheit bei Organisation und Informatik der Stadt Zürich (OIZ) tätig



lers ermittelt. Die Aufgabe bestand nun darin, den Loghost so zu konfigurieren, dass dieser alle Anmeldungen in Echtzeit auswertet und die Anzahl erfolgreicher Logins registriert. Auf diese Weise lässt sich die Zahl der an einem Tag angemeldeten Benutzer zu jedem Zeitpunkt herauslesen. Einmal täglich wird dieser Wert in «Stata9» importiert und induktiv bezüglich der Normwerte ausgewertet. Zudem hat die Stadtverwaltung verschiedene Filter auf dem Loghost implementiert:

- **Dublettenfilter:** Ein einzelner Benutzer kann sich mehrmals pro Tag anmelden, deshalb müssen Dubletten herausgefiltert werden.
- **Zeitfenster:** Es gibt viele Anmeldevorgänge, die nicht von Menschen ausgelöst werden. Diese spielen sich gehäuft in der Nacht ab. Deswegen berücksichtigt das Absenzen-Monitoring nur den Zeitraum zwischen 6:00 und 22:00 Uhr.
- **Automatische Logins:** Smartphones verursachen ohne Zutun des Benutzers Anmeldevorgänge für den E-Mail-Abwurf. Smartphone-Logins werden daher nicht gezählt, da sie keine Aussage über die Arbeitsfähigkeit des Mitarbeiters erlauben.
- **Heimarbeiter:** Angestellte, die sich via Internet von zu Hause anmelden, werden gezählt. Sie können normalerweise ihrer Arbeit nachgehen.

## ERSTE RESULTATE

Um Normwerte für die Anzahl der Logins zu errechnen, wurden bislang 18 Wochen ausserhalb der Ferienzeit analysiert – ohne die Werte der offiziellen Feiertage. An Dienstagen arbeiteten jeweils die meisten Angestellten. Die Auswertung (siehe Grafik links) konzentriert sich deshalb auf die Dienstage. Die Login-Zahlen während der sieben Ferienwochen 2009 liegen deutlich ausserhalb des Vertrauensintervalls. Das beweist die Zuverlässigkeit des Monitoring-Systems.

Die Lösung wurde im Übrigen auch vom Datenschutzbeauftragten gutgeheissen. Personenbezogene Auswertungen sind nicht möglich, da alle notwendigen Informationen vollständig anonymisiert werden.

## FAZIT: EINFACHE UND EFFIZIENTE LÖSUNG

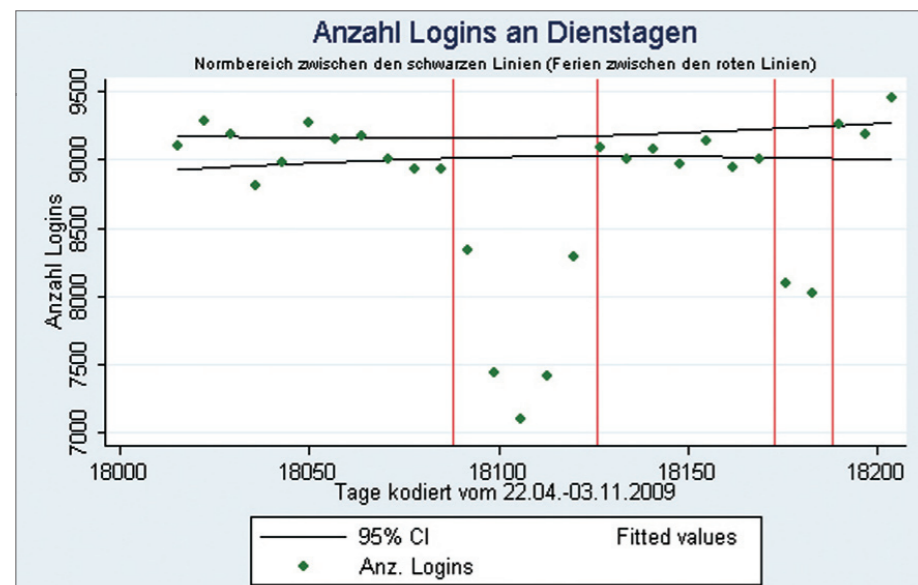
Die Stadtverwaltung Zürich hat mit verhältnismässig kleinem Aufwand ein zuverlässiges und alltagstaugliches Monitoring-Instrument zur Pandemieplanung implementiert. Das Beispiel zeigt eindrücklich auf, was mit der Sammlung und Auswertung von anonymisierten Login-Daten möglich ist: Vormalig unbedeutende Textmeldungen werden zu wertvollen Informationen für die Verwaltung.

Personenbezogene Auswertungen sind nicht möglich, da alle Informationen anonymisiert werden

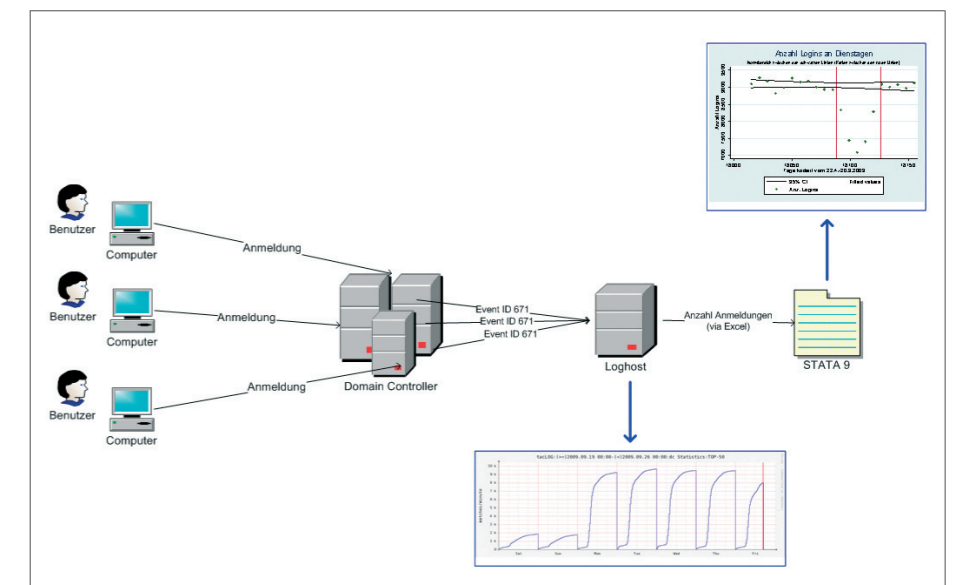
Um festzustellen, welche Bereiche des Grossbetriebs der Stadt Zürich von den Absenzen während einer Grippepandemie betroffen sind, müsste als nächster Schritt zum Beispiel

in vitalen Betrieben wie den Stadtspitälern nachgefragt werden, wie die jeweils aktuelle Auslastung der Belegschaft ist. Umgekehrt sind die Meldungen einzelner Dienstabteilungen über hohe Absenkraten auch im Kontext der gesamtstädtischen Abwesenheitsraten interessant.

Darüber hinaus unterstützt das Monitoring-Tool auch generelle Prognosen: Die Beobachtung der Krankenstandsentwicklung unter den Mitarbeitern einer grossen Firma, lässt Rückschlüsse auf den schweizweiten Verlauf einer Pandemie zu. Flankierend zu anderen epidemiologischen Daten, wie etwa Arztbesuche wegen Grippe pro 100 000 Einwohner und Grippekranken in den Spitälern, ermöglicht das neue Instrument daher auch Aussagen über Verlauf und Wendepunkt einer Grippepandemie in der Schweiz. ←



Frühwarnsystem: Abweichungen von «normalen» Fehlzeiten sind auf einen Blick erkennbar



Ablauf im Überblick: Die Login-Daten werden anonymisiert gesammelt und ausgewertet

BILD: FOTOLIA