ROGATOR
market research & software

Datensicherheits- und Datenschutzkonzept der Rogator AG

Stand: 10. April 2017

Rogator AG
Emmericher Straße 17
90411 Nürnberg

Vorstand: Johannes Hercher
Datenschutzbeauftragter: Dr. Axel Theobald

Relevante Komponenten des Konzepts:
A. Umfrageserver und Serverhousing
B. Interne Fileserver
C. Datentransfers
D. PC-Ausstattung
E. E-Mail-Verkehr
F. Anweisungen und Verhaltensregeln

A. Umfrageserver und Serverhousing

A1. Umfrageserver

Rogator betreibt zahlreiche Internet-Server zur Durchführung von Online-Befragungen und verwandten Dienstleistungen. Dabei handelt es sich um eigene Server der Rogator AG (Serverhousing noris network AG sowie M-net GmbH) und gemietete virtuelle Server (Serverhousing noris network AG). Alle Server werden ausschließlich von der Rogator AG konfiguriert und betreut:

- Performante Internet-Server mit wartungsarmen Linux-Betriebssystemen und unterbrechungsfreiem Lauf
- Verwendung bewährter und geprüfter Open Source-Komponenten
- Regelmäßige Logfile-Analyse der Server nach Auffälligkeiten
- Regelmäßige Sicherheits-Updates je nach Erscheinen
- Wartungsarbeiten per Ferndiagnose über verschlüsselten Zugang (Zugriff erfolgt ausschließlich über SSL VPN (über Firewall) und SSH)
- Alle Systemaktivitäten werden mittels Linux SysLog protokolliert
- Alle Nutzeraktivitäten werden durch die RogManager-Software protokolliert (z.B. Uploads, Downloads, Erstellen, Löschen, Zurücksetzen etc.)
- Abgestuftes Backup-System (täglich: inkrementell, wöchentlich: differentiell, monatlich: Vollbackup); Datenbestand liegt für max. 2 Monate als Backup vor
- Zusätzliches, externes Backup (täglich) über SSH-Verbindung auf dedizierten Rogator-Server bei Firma LeaseWeb Deutschland GmbH, Kleyerstraße 79, 60326 Frankfurt am Main
- Festplattenspiegelung (RAID-Systeme)
- Firewall

- Ständige Prüfung der Serververfügbarkeit
- Berechtigungssystem für Zugriffe auf Kundenaccount-Ebene
- Logische und teils physikalische Mandantentrennung (Lagerung von Umfragedaten der Kunden in voneinander getrennten Betriebssystemordnern bzw. auf verschiedenen Servern)
- Schriftliche Freigabe der Zugriffsberechtigung auf Masteraccount-Ebene durch Geschäftsführung und Datenschutzbeauftragten
- SSL-Verschlüsselung auf Wunsch verfügbar
- Verschlüsselte Ablage der Kundenaccount-Passwörter (kryptografische Hashfunktion „bcrypt“)
- Optionale Zusatz-Verschlüsselung der Ergebnisdateien beim Download

A2. Serverhousing 1

Für das Housing Rogator-eigener sowie gemieteter virtueller Server werden die Einrichtungen der Firma noris network AG, Thomas-Mann-Str. 16-20, 90471 Nürnberg mit optimaler Internetanbindung genutzt. Die noris network AG verarbeitet jedoch keine Daten für die Rogator AG (auch keine personenbezogenen) und hat keinen Datenzugriff.

Energieversorgung

- ≥ 99,991 % p.a. Verfügbarkeit für Energieversorgung
- AlwaysOn-Technologie für redundante USV-Versorgung von A- und B-Feed
- Notstrom über Dieselgeneratoren mit Treibstoffvorrat für mindestens 72 Stunden unter Volllast
- Während des Betriebes auffüllbare Dieseltanks (Nachbetankung vor Erreichen des Minimalfüllstandes gesichert durch 24/7-Liefervertrag)
- Redundante Anbindung an Energieversorger
- 100 % Nutzung regenerativer Energie mit RECS-Zertifikat

Klimatisierung

- Klimatisierung über KyotoCooling® (erlaubt mehr als 90 % des Jahres Kühlung ohne den hohen Energieverbrauch von mechanischen Kompressoren)
- ≥ 99,991 % p.a. Verfügbarkeit für Klimatisierung
- 100 % Trennung Kalt- und Warmbereich durch Einhausung und Warmluftseparierung über doppelte Decke

Netzwerkanbindung

- ≥ 99,991 % p.a. Verfügbarkeit des Backbones
- Mehrfach redundante und Carrier-neutrale Internetanbindung über eigenen multiplen 10 Gbit/s-Glasfaser-Backbone
- Gesamtkapazität der Internetanbindung 800 Gbit/s
- Anbindung an Layer-1 (DWDM/CWDM), Layer-2 (Ethernet/FC-AL/FICON) oder Layer-3 (IP/MPLS) möglich
- Redundante Anbindung an alle wichtigen Peering-Punkte

Brandschutz

- Flächendeckende Brandmeldeanlage mit Brandfrühesterkennung und direkter Aufschaltung zur Feuerwehr Nürnberg
- Zonengenaue Löschung mittels Stickstoff (N2) und anschließende zeitlich unbegrenzte Sauerstoffabsenkung durch OxyReduct®

- Einsatz von nichtbrennbaren oder nur schwer entflammbaren Materialien
- Bauliche Maßnahmen nach Feuerwiderstandsklasse F90

Sicherheit

- Videoüberwachung mit Archivierung
- Sicherheitsdienst vor Ort (24 h)
- Biometrische Zutrittskontrolle für 24/7-Zugang mit Transponderkarte
- Raum-in-Raum-Konzept trennt IT-Flächen von Außenwänden
- Perimeterschutz mit Sicherheitszaun und Vereinzelungsschleusen
- Rack-Überwachung mit leistungsfähigen Monitoring-Systemen
- Separate Cages innerhalb des Rechenzentrums mit eigener Absicherung, Zugangs- und Einbruchmeldesystem verfügbar

Weitere Leistungsmerkmale

- Zertifizierungen:
  - ISO 27001-Zertifizierung
  - ISO 20000-1-Zertifizierung
  - ITIL®-Zertifizierung
  - Zertifizierung nach ITGSK des BSI
- Auszeichnungen
  - 5 Sterne beim eco Datacenter Star Audit für Single Site und Interconnected Site
  - Internet Award für IT Infrastruktur
  - Grüner Stern für Approved Energy Efficient Datacenter
  - Deutscher Rechenzentrumspreis 2012 zusammen mit der Wagner Group
- Begehbare doppelte Decke anstelle von Doppelboden
- Modulares Konzept mit patentierten Combinded Energy and Cooling Cells
- Bis zu 18 kVA für alle Racks im Rechenzentrum (High Density-Racks)
- Verwendete Racks: 47 HE x 600 x 1200 (Größe des Drittel-Rack: 15 HE)

A3. Serverhousing 2

Für das Housing weiterer Rogator-eigener Server werden die Einrichtungen der Firma M-net Telekommunikations GmbH, Spittlertorgraben, 90429 Nürnberg mit optimaler Internetanbindung genutzt. M-net stellt lediglich die Konnektivität zum Internet her, verarbeitet jedoch keine Daten für die Rogator AG (auch keine personenbezogenen) und hat auch keinen Datenzugriff:

- Elektronisches Schließsystem mit Videoüberwachung
- Persönliche Zutrittskontrolle (elektronisch codierte Zugangskarte im Besitz von Rogator)
- Zutrittsbeschränkung für zwei registrierte Mitarbeiter von Rogator
- Abschließbare Serverracks
- Verschlossene Türen bei Abwesenheit
- Alarmanlage
- Brandmeldeanlage
- Unterbrechungsfreie Stromversorgung
- Überspannungsschutz
- Redundante Klimaanlage mit Doppelbodenbelüftung

B. Interne Fileserver

Die internen Fileserver der Rogator AG befinden sich in einem gesicherten, fensterlosen Raum in der Mitte der Bürofläche der Rogator AG:

- Verschlossene Türen bei Abwesenheit
- Schlüssel-/Chipregelung für den Serverraum
- Alarmanlage für Serverraum
- Hierarchisches Rechtesystem gewährt jedem Mitarbeiter nur Zugriff auf die benötigten Laufwerke nach dem Need-to-Know-Prinzip (teilweise auch nur Lesezugriffe)
- Berechtigungskonzept zur bedarfsorientierten Ausgestaltung der Zugriffsberechtigungen mit schriftlicher Freigabe durch Geschäftsführung und Datenschutzbeauftragten
- Entzug von Berechtigungen jederzeit mit sofortiger Wirkung möglich
- Personenbezogene Logins zur Autorisierung
- Passwort-Regeln etabliert (Länge, Komplexität etc.)
- Passwort-Änderung im 3-Monats-Rhythmus
- Sperrung bei dreimaliger Falscheingabe
- Firewall
- Kein Anschluss von betriebsfremden Rechnern an das Netzwerk
- Besonders zu schützende Daten werden nach Verarbeitung auf verschlüsselte Laufwerke gespielt (TrueCrypt)
- Pro Projekt Trennung der Daten in festgelegten Ordnern, die unterschiedlichen Zwecken dienen (z.B. Mailinglisten und Rohdatensätze)
- Backup-System mit täglicher Sicherung aller relevanten Laufwerke
- Zusätzliche Sicherungskopien mit Safe-Lagerung in separatem Gebäude (anderer Brandabschnitt)

C. Datentransfers

Für die Übertragung von Daten bzw. deren Transfer auf Datenträger gelten folgende Prinzipien und Maßnahmen:

- Einsatz von Verschlüsselungsverfahren (SSL, VPN, SSH)
- Aufbewahrung von Datenträgern in verschließbaren Schränken (Data Safes)
- Nutzung von Datenträgern an den Arbeitsplätzen technisch verhindert (CD-ROM, USB-Stick, Disketten etc.)
- Datenträger (z.B. USB-Stick, CD-ROM) können lediglich über die Logins/PCs der Teamleiter bzw. unter deren Kontrolle angeschlossen werden
- Verwendung von verschlüsselten USB-Sticks
- Richtlinien für die Übertragung von Kundendaten (Adresslisten, Datensätze von Umfragen, Auswertungen etc.): Verwendung einer Verschlüsselung oder Benutzung der SSL-Download-Plattform

D. PC-Ausstattung

Bezüglich der Arbeitsplatzrechner der Rogator AG sind folgende Regeln getroffen:

- Passwort-Änderung im 3-Monats-Rhythmus
- Begrenzung der Fehlversuche beim Windows-Login: Sperrung bei dreimaliger Falscheingabe

- Passwort-Regeln etabliert (Länge, Komplexität, keine Trivialpasswörter, signifikante Änderung bei turnusmäßiger Neuvergabe etc.)
- Dunkelschaltung des Bildschirms nach 3 Minuten mit Passwortschutz
- Manuelle Bildschirm- bzw. Rechnersperrung bei Verlassen des Arbeitsplatzes
- Windows-Firewall
- Ständig aktualisierte Virenscanner, regelmäßige Scans
- Ausschluss/Verbot der eigenständigen PC-Einrichtung/-Anpassung durch Mitarbeiter
- Software-Installation nur nach Freigabe durch System-Admin oder Geschäftsführung
- Stichprobenartige Prüfung der PCs
- USB-Anschlüsse / CR-ROM-Laufwerke deaktiviert, Freigabe durch Geschäftsführung und Datenschutzbeauftragten
- Deaktivierung von Browserfunktionen zur automatischen Speicherung von Account-Passwörtern

E. E-Mail-Verkehr

Für die Verwendung von E-Mail gelten die folgenden sicherheitsrelevanten Regulierungen:

- Passwort-Regeln für E-Mail-Postfächer etabliert (Länge, Komplexität, etc.)
- Passwort-Änderung im 3-Monats-Rhythmus
- Administration der Postfächer durch max. drei Personen im Unternehmen
- Schriftliche Freigabe der Administration durch Geschäftsführung und Datenschutzbeauftragten

F. Anweisungen und Verfahrensregeln

Neben den technischen Voraussetzungen sind bei der Rogator AG die folgenden, sicherheitsrelevanten Aspekte schriftlich niedergelegt. Die entsprechenden Regelungen sind an alle Mitarbeiter kommuniziert und darüber hinaus jederzeit zugänglich:

F1. Allgemeines

- Bestellung eines Datenschutzbeauftragten und Meldung bei den zuständigen Behörden
- Regelmäßige Hinweise und Ermahnungen bzgl. der Datenschutzproblematik zur Förderung des Problembewusstseins
- Unangekündigte In-House Kontrollen bezüglich der Einhaltung der Datenschutz- und Datensicherheitsmaßnahmen durch den Datenschutzbeauftragten
- Kommunizierte und jederzeit zugängliche Datenschutzbestimmungen
- Schriftliche Geheimhaltungsverpflichtung mit allen MitarbeiterInnen
- Schriftliche Bestätigung der Kenntnisnahme der einschlägigen Bestimmungen des Datenschutzgesetzes (BDSG)
- Verpflichtungserklärung zum Fernmeldegeheimnis i.S.d. § 88 TKG
- Schriftliche Bestätigung der Kenntnisnahme der internen Datenschutzbestimmungen von allen Mitarbeitern der Rogator AG
- Schriftliche Freigabe öffentlich verwendeter Dokumente (z.B. Vertriebspräsentationen, Demoauswertungen etc.) durch Geschäftsführung und Datenschutzbeauftragten
- Regelung für den Zutritt nicht-zutrittsberechtigter Personen (z.B. Geschäftskunden, Besucher etc.)
- Besetzung des Empfangs (zu den Bürozeiten)

- Einbruchssichere Brandschutztür mit Alarmanlage
- Regelungen für die Vernichtung von Datenträgern (z.B. CD-ROMs) über Spezialfirma (mit Vertrag zur ADV)
- Regelung zur Vernichtung von Papiermüll (Aktenvernichter mit entsprechender Norm)
- Regelkreis zur Behandlung von technischen Problemen (Incident Management)
- Speicherung von Projektdaten und Arbeitsergebnissen ausschließlich auf Netzlaufwerken mit täglichem Backup (nicht auf PCs selbst)
- Abschluss von individuellen Datenschutzvereinbarungen mit den Kunden
- Weitergabe von Admin- oder Masterpasswörtern ausschließlich durch die Geschäftsführung
- Weitergabe von Zugriffsrechten an Auftraggeber nur im erforderlichen Umfang (z.B. nur Infokonto bei Full Service-Projekten)
- Büroräume im 2. Obergeschoss, keine Feuerleiter oder Feuertreppe (keine Einstiegsgefahr durch Fenster)
- Zeiterfassungssystem für Mitarbeiter
- Rauchverbot in Büroräumen (insb. in Serverräumen)

F2. Umgang mit sensiblen, insb. personenbezogenen Daten

- Personenbezogene Daten werden nur dann verarbeitet, wenn dies unbedingt erforderlich ist
- Arbeiten mit Schlüssellisten und Prinzip der Datentrennung
- Kein Aufspielen personenbezogener Daten auf die Umfrageserver (anonyme Codelisten)
- Archivierung von Mailingdaten und Schlüssellisten nach Projektabschluss auf verschlüsselten Laufwerken (TrueCrypt)
- Richtlinien für die Übertragung von Kundendaten (Adresslisten, Datensätze von Umfragen, Auswertungen etc.): Verwendung einer Verschlüsselung oder Benutzung der SSL-Download-Plattform
- Richtlinien für verwendete Passwörter
- Mitteilung von Passwörtern an Auftraggeber ausschließlich per Telefon
- Herausgabe von Umfragedaten oder Auswertungen ausschließlich an bekannte und berechtigte Personen beim Auftraggeber
- Löschen von Schlüssellisten nach Projektende auf Anforderung

F3. Datenschutzerklärung / Vereinbarung zur Auftragsdatenverarbeitung

In Form von gesonderten Datenschutzerklärungen können die von Rogator ohnehin standardmäßig durchgeführten Maßnahmen und Prinzipien auch schriftlich vereinbart werden:

- Auftraggeber ist „Herr der Daten“
- Namentliche Festlegung von weisungsbefugten Ansprechpartnern auf beiden Seiten
- Berufung auf das Bundesdatenschutzgesetz
- Keine anderweitige Verwendung der Daten durch den Auftragnehmer
- Keine Überlassung der Daten an Dritte
- Umgang mit Ausschussmaterial (Löschung, Vernichtung, Rückgabe)
- Verpflichtung der Mitarbeiter auf das Datengeheimnis sowie Fernmeldegeheimnis (§ 88 TKG)
- Bestellung eines Datenschutzbeauftragten
- Löschen der Daten nach Auftragsabwicklung auf Anweisung
- Einverständniserklärung zur Kontrolle vor Ort
- Zustimmung zur Erteilung von Unteraufträgen