Who we are and what we do for you …

Software development.
IT-security consulting.
Innovation.

Who we are …

Digitronic® computersysteme gmbh (headquarters in Chemnitz) has been creating IT-solutions in the fields of communication and digital confidentiality since 1991. With a clear focus on reliability, customer-friendly service and functionality, our team creates innovative software solutions. We are software developers and service providers with a passion. Regardless of the type of challenge you present us with: We focus on finding a solving the problem.

With more than 25 years of experience, we are firmly established as a software developer, well-connected, working together with competent partners. Mobile, platform-independent confidentiality in conjunction with smartphone technology that can also be used in the Industry 4.0 environment – this is a current focus of research and development in close collaboration with major customers. digitronic® is the regional office of the Bundesverband IT-Sicherheit e.V. TeleTrusT and bears the seal 'IT-Security made in Germany'.

What we do …

Our role is to protect your data in such a way that the confidentiality of sensitive data is strengthened within existing information security concepts. That is why, for more than 15 years, we have been developing and marketing successful products and solutions for convenient and secure log-on to operating systems as well as for encrypting confidential data on network drives.

Our **All-In-One Security Packages** combine these technologies with support services at your premises. We support you not only in all the necessary analyses and development of solutions but also during test installations and implementation steps. In this way the requirements of 2-Factor-Authentication and Team encryption as part of the certification in accordance with ISO 27001, auditing processes in accordance with VDA ISA and other tests of information security with our customers have already been fulfilled a hundredfold. We turn our expertise into added value for you and your company.

Our contribution to you in the automotive sector…

Automobile suppliers must have their information security tested in accordance with **VDA ISA** when they exchange prototypes and data regarding development and construction with automobile manufacturers. As of 2017, tests of this nature take place with various manufacturers under the auspice of the ENX Association through/over **TISAX**. It's no longer only/just about access to construction data and administration systems (KVS) of Volkswagen, but rather/instead about access to sensitive data of all European OEMs.

In accordance with the test criteria of the VDA ISA, not only the procedures for secured access to networks, applications and data but also for encryption of information during storage and transport are to be implemented. There we support you with solid solutions that have been tried and tested, matured and further developed over 15 years, both for encrypting sensitive data on network drives as well as for secure and convenient log-on to the operation systems and applications.

On the following page you can see a list of the controls of the VDA ISA we can support you with using our recognized solutions.

VDA ISA–Controls and our All-In-One-solutions

Control 9.1 (Access Control - access to the IT-systems)

Added when a very high level of protection is required:

+ Data requiring a very high level of protection must be secured by way of a strong authentication (e.g. 2-Factor-Authentication).
  Our powerful 2-Factor-Authentication enables a secure and convenient log-on to operating systems. The Tokens used are certified in accordance with EAL 4+ (Common Criteria) and thereby fulfill the requirements.

Control 9.5 (Access Control - access to information and applications)

Added when a very high level of protection is required:

+ Encrypted storage of data to prevent access and spying by unauthorized persons /entities (e.g. Administrators) at file level.
  By way of a separate user-management system, our encryption method makes it impossible for unauthorized persons or entities, including administrators, to gain access to the information to be protected. This level of protection can be increased: authorized users must then prove their identify by way of a 2-Factor-Authentication in the encryption solution.

Control 10.1 (Cryptography)

Added when a high level of protection is required:

+ The following aspects must be documented:

  - Description of the key control
  With the help of the separate user administration of our encryption solution the sole sovereignty over the distribution of keys will be assigned to one responsible person/entity (or to several responsible persons/ entities) for the security of the information to be protected.

  - Control of the administration of the key material in the case of external processing (e.g. in the Cloud)
  The control/sovereignty of the administration/management of the key material always rests with the person responsible for the security of the information, regardless of whether the data is saved on internal or external servers.

  Information requiring a high level of protection should be sent or transmitted encrypted.

  Our client-based encryption of data stored on network-drives always encrypts and decrypts the information to be protected at the Client. In this way the data is always transported and sent in encrypted form.

Added when a very high level of protection is required:

+ Information with a very high level of required protection **is stored encrypted**.
  Our encryption solution implements encrypted storage of the information needing protection with secure and recognized/approved procedures/methods.

Your point of contact

digitronic® computersysteme gmbh
Oberfrohnaer Str. 62
09117 Chemnitz

Tel: +49 371 81539 0
Fax: +49 371 81539 900
E-Mail: vertrieb@digitronic.net
Internet: www.digitronic.net