Feedback (Suggestions for improvement): English version

4096-bit encryption/Elliptic Curve Cryptography (logon encryption types)/Two-factor authentication/Transport Layer Security (TLS protocol)/Full IPv6 support/HMAC authentication/ Cipher Block Chaining/Diffie-Hellman key exchange/Station-to-Station (STS) protocol/ Pretty Good Privacy/Perfect Forward Secrecy/Encryption Tool (CloudStorage/Backup)/ Failure Backup Solution/NAT Firewall/DDoS protection service/Load Balancing/DNS Leak/ IP Leak/WebRTC Leak/Windows Login Leak/Artificial Intelligence (NeuroRouting™)/ Zero knowledge proof/Fiat Shamir protocol/Schnorr identification/SecureCore function (security kernel)/Web cleaner function (system cleanup)/Gutmann method (complete data deletion)/Device backup function (cloud storage)/Memory protection function (protection against server failures)/Server failure (protection options)/Optional: New Payment Methods/Bonus: company pension scheme (for all employees)/Bonus: occupational disability insurance/Bonus: Supplementary health insurance/Cafeteria-Modell (Cafeteria plan)/ Bonus: Company social benefits

Please forward the suggestions to the responsible departments (**technical department/Webhosting Provider/Programming department**). For the forwarding I thank you in advance.

4096 bit encryption:
https://www.pcwelt.de/ratgeber/Verschluesselung_-_Was_ist_noch_unknackbar_-Sicherheits-Check-8845011.html
https://www.heise.de/security/artikel/Kryptographie-in-der-IT-Empfehlungen-zu-Verschluesselung-und-Verfahren-3221002.html?seite=all
These are recommended for encryption.

Highly Secure Elliptic Curve Cryptography (Login Encryption Types):
https://de.wikipedia.org/wiki/Elliptic_Curve_Cryptography
https://www.heise.de/select/ix/2017/3/1487529933065685
https://www.computerweekly.com/de/definition/Elliptische-Kurven-Kryptografie-Elliptic-Curve-Cryptography-ECC
https://www.globalsign.com/de-de/blog/ecc-101/
https://www.ssl247.de/certificats-ssl/rsa-dsa-ecc

For the customer area these are ideally suited.

Two-Factor Authentication (TOTP):
https://de.wikipedia.org/wiki/Zwei-Faktor-Authentisierung
https://www.pcwelt.de/ratgeber/Wichtige_Dienste_per_Zwei-Faktor-Authentifizierung_schuetzen-Sicherheit-8679969.html
https://www.security-insider.de/flexiblere-zwei-faktor-authentifizierung-an-vpns-a-700259/
https://www.security-insider.de/remote-access-vpn-mit-zwei-faktor-authentifizierung-a-389000/
http://www.itseccity.de/produkte-services/it-security/vpn-loesungen/ncp-engineering090315.html
The customer accounts are doubly secured by the Two-factor authentication and therefore very difficult to hack.The activation of the Two-factor authentication is voluntary (option in the customer account). When you use Two-factor authentication activated, you need to login to the desktop version (PC) always the authenticator app.

Authenticator app:
a) FreeOTP Authenticator/b) Authy/c) Microsoft Authenticator/
d) Lastpass Authenticator/e) Google Authenticator
Two-factor authentication is immediately active and armed. The next time you log in, the 6-digit code must be used when calling the Authenticator App for the customer account is displayed in the field provided for this purpose (authenticator code).

Transport Layer Security (TLS protocol): 1.3. Version, etc.
https://en.wikipedia.org/wiki/Transport_Layer_Security
https://de.wikipedia.org/wiki/Transport_Layer_Security
Transport Layer Security, more commonly known under the previous name Secure Sockets Layer, is a hybrid encryption protocol for secure data transmission on the Internet. If the connection is encrypted using SSL/TLS, it is almost impossible for anyone to read the online traffic.

Full IPv6 support:
This means that users will automatically receive an IPv6 address in addition to the normal IPv4 address after establishing an Internet connection. This gives you full access to the IPv6 network. In addition, full IPv6 integration also means that all users are automatically protected from IP leaks via IPv6. This provides full connectivity and future viability, since many mobile networks no longer allocate IPv4 on their own (cgNAT could slow down the connection speed).

These are recommended for safety reasons.

HMAC authentication: https://en.wikipedia.org/wiki/HMAC
HMAC stands for keyed-hash message authentication code. A message authentication code is a protection against the modification of transmitted data by an attacker who receives the data can read in real time. TLS hash values (hence the H in HMAC) from the many ways to reliably authenticate messages.

Cipher Block Chaining: https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#CBC
CBC stands for Cipher Block Chaining, which is every message depending on the previous passes. So can yourself short interruptions of the channel can be quickly noticed.

Diffie-Hellman key exchange: https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange
A symmetric encryption scheme is used, the key of which is the negotiation of Diffie-Hellman key exchanges with elliptic curves. The server and the app use intelligent math to negotiate and verify the secret key, which is then used to encrypt the entire session's data.

Station-to-Station (STS) protocol: https://en.wikipedia.org/wiki/Station-to-Station_protocol
In public-key cryptography, the Station-to-Station (STS) protocol is a cryptographic key agreement scheme. The protocol is based on classic Diffie–Hellman, and provides mutual key and entity authentication. Unlike the classic Diffie–Hellman, which is not secure against a man-in-the-middle attack, this protocol assumes that the parties have signature keys, which are used to sign messages, thereby providing security against man-in-the-middle attacks. In addition to protecting the established key from an attacker, the STS protocol uses no timestamps and provides perfect forward secrecy. It also entails two-way explicit key confirmation, making it an authenticated key agreement with key confirmation (AKC) protocol.

Pretty Good Privacy: https://en.wikipedia.org/wiki/Pretty_Good_Privacy
PGP encryption uses a serial combination of hashing, data compression, symmetric-key cryptography, and finally public-key cryptography; each step uses one of several supported algorithms. Each public key is bound to a username or an e-mail address. The first version of this system was generally known as a web of trust to contrast with the X.509 system, which uses a hierarchical approach based on certificate authority and which was added to PGP implementations later. Current versions of PGP encryption include both options through an automated key management server.

Perfect Forward Secrecy: https://en.wikipedia.org/wiki/Forward_secrecy
With Perfect Forward Secrecy, even if a dedicated opponent is somehow able to attack the computer or server during a session, they will not be able to decode traffic from past sessions. The provider uses namely with each connection a new secret key. Even if you stay connected to the provider for a long period of time, the provider automatically changes the key every 60 minutes. This key renewal process every 60 minutes guarantees "forward secrecy". So if an attacker succeeds in compromising the key, in the worst case scenario, he could track the data for up to 60 minutes. Then everything is secret again.

Encryption Tool (Cloud Storage/Backup): https://nuetzlich.net/gocryptfs/
With the Locker App you can save your data within seconds with end-to-end encryption. Drag and drop into a vault folder and you're done. GoCryoptFS requires a locker key to open and close a lock. When a locker is applied, a 256-bit key is generated using Libsodium. Thereafter, this Locker key is still encrypted with XSalsa20-Poly1305 MAC using a secret key (this is assigned to one when setting up the account). Now the locker key is secured and the file can be encrypted. This is done using AES-GCM for file content encryption and EME for file name encryption. To gain access to the files in the vault, the user must set a master password. Every time you want to open your vault, you need this password. It should be easy to remember, as you will often need it. The master password is also important for encryption of the secret key. The user is the only one who knows the master password. It is not stored in the app or on the servers in order not to be hacked. If you forget or lose your master password despite its importance, you can reset it with the so-called recovery key.
This recovery key is obtained as an emergency tool during registration.

Advantages:
1.) Encryption with just one click
2.) Ability to reset the master password
3.) Possible with any file type and size
4.) Encrypts the data stored locally on the computer as well as those in the cloud
5.) Access on multiple devices
6.) App available for macOS and Windows
7.) Strong encryption systems (Argon2, AES-256, ECC)
8.) Easy to use & user friendly

Failure Backup Solution:
An Automatic Failure Backup solution within each country. Through an intelligent control system, in case of failure of a server the provider connection automatically and without delay another location in the same country. Connection interruptions are thereby excluded.

NAT Firewall:
NAT Firewall is an additional layer of security for your internet connection. It blocks unsolicited inbound traffic when connected to the provider. There is no additional configuration or software is required because of it running on the servers. NAT Firewall protects any device connected to the provider.

DDoS protection service:
https://en.wikipedia.org/wiki/Denial-of-service_attack#Distributed_attack
https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/
https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html
https://www.digitalattackmap.com/understanding-ddos/

The DDoS protection service is capable of even the most complex ones Ward off DDoS attacks.

Load Balancing:
https://de.wikipedia.org/wiki/Lastverteilung_(Informatik)
https://www.nginx.com/resources/glossary/load-balancing/

Load balancing often goes hand in hand with mechanisms for fail safety: By building a cluster with the appropriate capacity and distributing the requests to individual systems, you can increase the fail safety if the failure of one system is detected and the requests are automatically submitted to another system.

DNS Leak:
Own DNS server without records (RAM-disk). In addition, OpenDNS servers (IPv6) are used (Choice in the settings). The service protects reliably before the known DNS leak.
https://www.hongkiat.com/blog/creating-ram-drives/
https://www.tomshardware.com/news/what-we-know-ddr5-ram,39079.html
https://www.opendns.com/about/innovations/ipv6/

IP Leak:
Its own software reliably prevents attacks known DNS leak methods.

WebRTC Leak:
The service reliably protects against the well-known WebRTC leak problem.

Windows Login Leak:
The service reliably prevents the sources of danger of the Windows login leak.

Artificial Intelligence (NeuroRouting™):
NeuroRouting™ is almost like a cascade of two servers, only automatic and intelligent and not end-to-end, respectively encrypted point to point. What makes the most sense depends on the intended use. Eternally long cascades make it slow to send data halfway around the world speeds up nothing. Usually NeuroRouting™ is enough, with a cascade with two servers. Based on Google's open-source library for machine learning (TensorFlow),a network can be minimized (https://en.wikipedia.org/wiki/TensorFlow).

The intelligent systems from the provider recognize where the target of each data is based on a self-adjusting database. In this case, the logics, which also develop themselves further, decide within a few milliseconds via which server the data should leave the global server network so that they can be securely transmitted over the entire route. Several server locations are also combined with each other (cascading). Because this happens every time you transfer data, even web pages that come from content from multiple sources are even retrieved across multiple locations. This happens fully automatically and in most cases speeds up the data transfers and in any case makes it impossible to predict the routes of the data from the outside. Therefore, even a globally organized monitoring possibility of the data is completely excluded.

Artificial Intelligence (NeuroRouting™) offers the following benefits:
1.) Selects the closest server to the destination
2.) Data traffic remains as long as possible in the encrypted server network
3.) External IP address changes depending on the destination
4.) In the ideal case, the data traffic does not appear on the Internet at all
5.) The number of attack points is minimized
6.) Complicates the tracking considerably
7.) Dynamic: The algorithm "learns" and responds to changes

Zero knowledge proof:
https://en.wikipedia.org/wiki/Zero-knowledge_proof
https://de.wikipedia.org/wiki/Zero-Knowledge-Beweis
A zero-knowledge proof (also knowledge-free proof) or zero-knowledge protocol (also knowledge-free protocol) is a protocol from the field of cryptography. In a zero-knowledge protocol, two parties (the verifier and the verifier) communicate with each other. The verifier is likely to convince the verifier that he knows a secret without revealing any information about the secret itself.

Fiat Shamir protocol:
https://en.wikipedia.org/wiki/Feige%E2%80%93Fiat%E2%80%93Shamir_identification_scheme
https://de.wikipedia.org/wiki/Fiat-Shamir-Protokoll
The Fiat Shamir protocol is a cryptographic protocol that can be used to authenticate yourself to someone. It shows that you know a square root (private key) of a previously published square number (public key). The method only reveals a single bit of the private key, namely the sign.
A variant is the Feige-Fiat-Shamir protocol, in which no information about the private key is disclosed. One therefore speaks of a zero-knowledge protocol. In particular, the protocol is perfectly zero-knowledge. This means that there is a simulation algorithm that generates a transcript in polynomial time that cannot be distinguished from a real interaction.

Schnorr identification:
https://en.wikipedia.org/wiki/Schnorr_signature
https://de.wikipedia.org/wiki/Schnorr-Signatur
The security is based on the complexity of the discrete logarithm in finite groups. In cryptology, special cryptological hash functions are used, which additionally require that it is practically impossible to find collisions on purpose.

SecureCore function (security kernel):
By "SecureCore" it is meant that data that runs between the servers also occur via their own Internet connections. So that the users who now connect to server B, are previously connected to A. Its encrypted connection to server B is used. Technically ok, because individual connections on the Internet can no longer be tracked, as they are routed over existing Internet data connections. This is undoubtedly an advantage that can also be cited as a measure against mass surveillance and even against targeted surveillance. The Secure Core architecture allows to protect the users from network attacks that other Providers cannot defend against. A classic setup involves a client passing traffic through a server enroute to the final destination. If an attacker can get control of the server, or monitor the network of the server, they will be able to match clients with their traffic, nullifying the privacy benefits of the provider.

Web cleaner function (system cleanup):
This function mainly removes unused and temporary files. The history of visited websites and various other histories, such as recently used files or entered search terms for Windows search can also be cleaned up. In addition, it can remove errors and remaining entries after uninstalling programs from the Windows registry. With the help of various deletion methods such as the Gutmann method, it can irrevocably delete both sensitive files and entire data carriers. These measures are intended to speed up the system and protect the user's privacy.

Gutmann method (complete data deletion):
https://en.wikipedia.org/wiki/Gutmann_method
https://de.wikipedia.org/wiki/Gutmann-Methode

Is a method of completely deleting data stored on magnetic storage media, e.g. B. hard drives are stored.

Device backup function (cloud storage):
With the device backup function, you have the option of like photos, videos and contacts from the local device directly in the Back up cloud storage and restore it if necessary. Depending on the operating system, the data can be restored in the folder and file structure previously used.
A new button should be installed in the settings („Device backup function in cloud storage").

Memory protection function (protection against server failures):
This function is able to divide up the available working memory and to separate running programs from each other in such a way that a programming error or crash of a single program does not affect the stability of other programs or the overall system (memory protection mechanism).

Server failure (protection options):
Undervoltage protection (UVP)
Surge protection (OVP)
Short circuit protection (SCP)
Overload protection (OPP)
Overcurrent protection (OCP)
Overheating protection (OTP)
Japanese 105° C capacitors (lifespan of the power supply)
Fire detector (installed in the server room)

These protective functions (power supply) can prevent most server failures.

Optional: New payment methods
Amazon Pay, Credit Cards, PayPal, Sofortüberweisung, Bitcoin, Vouchers (Starbucks) and PaySafeCard, Skrill, Webmoney, Plimus, Payza, Cherry Credits, Mercado, Pago, Raekc, MyCard, Indomog, Pagseguro, Fanapay, Qiwi, Interac, Sofortüberweisung, Przelewy, Dotpay, iDeal, Alipay, Giropay, E-Prepag, SanalPara, PostaCeki, ToditoCash, Ukash, CashU, Phone Payment, Fortumo, Gudang Voucher, MOLPoints, Ecopayz, Necard, Gamania, Neosurf, GSCash, Ticket Surf, All o Pass, SMS Coin, MicroOdeme, ImpulsePay, DaoPay, Bank Transfer, Mobile Payment, SEPA direct debit authorization (with a right of withdrawal), Purchase on account (14 days payment term) and cash on delivery in Austria, Germany, Switzerland

Bonus: Company pension scheme (for all employees):
https://www.pensionsadvisoryservice.org.uk/about-pensions/pensions-basics/workplace-pension-schemes
https://de.wikipedia.org/wiki/Betriebliche_Altersversorgung

This is recommended for all employees (workers/employees). The statutory pension is not secure (further cuts will follow).

Bonus: occupational disability insurance (for all employees)
https://www.gocompare.com/health-insurance/disability-insurance/
https://www.versicherungen.at/berufsunfaehigkeit-versicherung-rechner/

Disability can affect anyone in the course of their working life. Most of the time it occurs completely unexpectedly and turns the previous life upside down. Those who can no longer pursue their profession due to physical or psychological restrictions lose their income and the previous standard of living can no longer be maintained.

Bonus: Supplementary health insurance (for all employees)
https://h4i.nl/health-insurance-and-cost/supplementary-health-insurance/
https://www.versicherungen.at/krankenzusatzversicherung/

Company health insurance is recommended for all employees. Most people in the world do not have health insurance.

Cafeteria model (cafeteria plan): for all employees
https://ceopedia.org/index.php/Cafeteria_system
https://de.wikipedia.org/wiki/Cafeteria-Modell

A cafeteria model is a form of a compensation model in human resources. The intention of this model is to increase motivation through individual choices. The system can be assigned to the cognitive theories of motivation.

Company social benefits:
Company social benefits are benefits from employers to employees or company pensioners or their relatives, which are paid in addition to the regular wages.
https://www.nibusinessinfo.co.uk/content/business-benefits-corporate-social-responsibility
https://dothegap.com/blog/en/5-examples-of-social-benefits-for-businesses/
https://consciouscompanymedia.com/workplace-culture/hr-innovations/6-ways-corporate-social-responsibility-benefits-employees/
https://officevibe.com/blog/socially-responsible-companies
https://de.wikipedia.org/wiki/Betriebliche_Sozialleistungen
https://www.jobware.de/Karriere/Betriebliche-Sozialleistungen.html